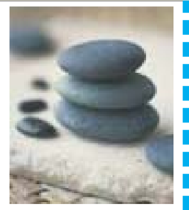






n°5
FEBRERO
2004

## Redes y sus Componentes básicos



Conozca los elementos básicos en los que se basan las redes de computadoras hoy.

## Suplemento de Seguridad



Guía de Certificaciones en Seguridad, Snort para Linux, Linux con la lupa en la seguridad, Ethical Hacking y más.

## Null Sessions o anonymous login



¿Qué podemos hacer para que nuestros sistemas sean un poco más difíciles de hackear?
Conocer, conocer y saber más.

# IT SECURITY










Febrero 2004, NEX saldrá mensualmente a partir de éste número.

Esto se debe a la repercusión que ha tenido y los pedidos que nos han hecho. Los temas seguirán siendo artículos con descripciones de mucho nivel de todos los temas que gobiernan hoy el mundo de Networking y Programación. Básicamente, sobre las tecnologías a las que se encuentra expuesto día a día el profesional de IT, o quienes estén realizando estudios avanzados.

Esto no quiere decir que no habrá introducción a temas. Por el contrario, éstos en particular intentarán darnos el "big picture" de cada temática.

NEX contendrá a partir de éste número un suplemento de Seguridad Informática. En particular NEX5 abarca casi exclusivamente este tema. Hemos inaugurado además, en conjunto con dos grupos de investigación del CONICET, un laboratorio de prueba donde analizaremos productos del mercado. De este modo daremos un exhaustivo análisis de lo bueno y no tan bueno de cada producto.

En la mayoría de los casos se hará una comparación entre las distintas opciones del mercado. Finalmente los temas educación y salida laboral seguirán teniendo gran prioridad.

Como siempre los invitamos a enviarnos comentarios y/o sugerencias. Aquellos interesados en colaborar con artículos o ideas son siempre bienvenidos,para ello deben contactarse a: articulos@nexweb.com.ar




## Staff

Año 3 Nº 5 2004

**Director**
Dr. Osvaldo Rodríguez

**Propietarios**
COR Technologies S.R.L.

**Coordinador Editorial**
Carlos Rodríguez Bontempi

**Cordinación General**
María Lujan Zito

**Responsable de Contenidos**
Dr. Osvaldo Rodríguez

**Editor en Jefe**
Raúl Kuzner

**Redactores**
Martin Sturm, Javier Pierini, Raúl Kuzner, Osvaldo Rodriguez, Maria Lujan Zito, Leonardo Posta, Paola Cuenca, Hugo Cela

**Humor**
Marcos Severi

**Distribución**
Lorena De Lillo, Ximena Antona

**Diseño Web SIte**
Emanuel A. Rincón

**Diseño Gráfico**
Carlos Rodríguez Bontempi

**Publicidad**
Ximena Antona
publicidad@nexweb.com.ar
4312-7694

**Preimpresión e Impresión**
Edigráfica S.A. Tel:4846236

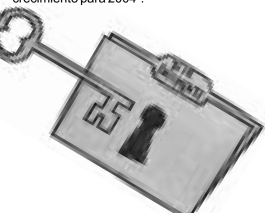
Periódico de Networking
Registro de la propiedad Intelectual en trámite leg3038

Dirección: Córdoba 657 12°Capital Federal
Tel:(011) 4312-7694 http:// www.nexweb.com.ar


El staff de Nex colabora ad-honoren, si desea escribir para nosotros enviar un e-mail a: articulos@nexweb.com.ar

Retire su ejemplar NEX en forma gratuita en Córdoba 657 piso 12° Capital Federal o solicítelo telefónicamente para su empresa al (011) 4312-7694 http:// www.nexweb.com.ar





# Redes, sus elementos fundamentales y seguridad

**En este artículo veremos un panorama general de los elementos básicos en los que se basan las redes de computadoras hoy. Muchas tecnologías entran en juego y durante las próximas apariciones de NEX discutiremos detalles de cada una de ellas.**

(Para complementar éste artículo los invitamos a ver una excelente presentación en video (de 12 minutos) donde se ejemplifica todo el proceso de uso de TCP / IP en redes). (download: www.warriorsofthe.net)

**1- Qué beneficio obtenemos en tener una red?**

Respuesta: Tener máquinas en red nos ayuda resolver un gran número de problemas.
El fin último de cualquier proyecto de redes es la de proveer algún tipo de servicio. Ejemplos:
-Necesito ver la página web de Ovis Link para conocer los precios de routers, hubs, switches, productos wireless. Existe un Web Server que aloja las páginas del dominio ovislink.com
-Necesito enviar un e-mail. Deberá existir un mail server y deberé ejecutar una aplicación cliente que me envíe y reciba una posible respuesta.
-Necesito compartir archivos y carpetas a toda mi empresa. Y, que estén en un solo server (file server) de modo de centralizar los back-ups.
-Necesito comprar una flauta travesera de plata: www.ebay.com y tipear ¨traverse flutes¨.

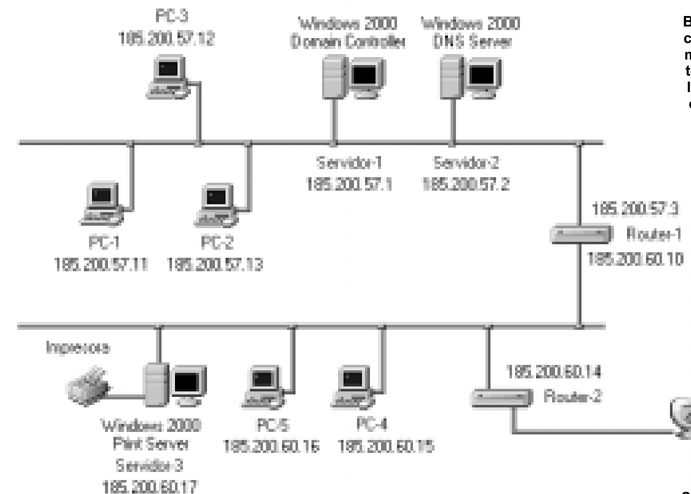
**2. Cuáles son los elementos fundamentales en una red ?**

**A. Todo tipo de servicio de red necesita un server-software y un client-software.**
**Relación ¨cliente servidor¨ entre maquinas.**

Conectamos las máquinas en red con un propósito: la computadora que actúa como cliente se beneficia de las computadoras que actúan como servidores: (ver figura)

-En la maquina cliente debe correr un programa que sepa solicitar un servicio y saber como recibir y mostrar lo que recibió: "aplicación cliente"
-Necesito en el servidor un programa que esté atento y sepa escuchar pedidos y enviar la información solicitada: "aplicación servidor"
Un ejemplo muy popular es el de Web browser (cliente) web server (servidor):
Si quiero ver la página web del periódico NEX utilizo mi "web-browser" (cliente web) y en algún lugar tipeo: http://www.nexweb.com.ar (http hipertext transfer protocol, es el protocolo que permite transferir hipertexto)
He dicho a la red: "quiero la página web de www.nexweb.com.ar que esta alojada en algún servidor." En nuestro caso no está en las oficinas de NEX sino en un proveedor de web-hosting (towebs)
Los paquetes saben encontrar donde esta el servidor. Cómo?

Se lo preguntan al servidor DNS: "cuál es el número IP del servidor (llamado www) que aloja la página web de nexweb.com.ar". DNS devuelve el IP correcto y los paquetes con el pedido viajan hasta la máquina con ese IP. El web-server (servidor) que está constantemente "escuchando" (tiene corriendo un pequeño programa llamado daemon, demonio), toma el pedido y envía, por ejemplo, el archivo index.html. El cliente lee el html y me lo muestra en pantalla
***Web-browsers más conocidos*: netscape, mozilla , internet explorer.**




***Web-servers más conocidos*: apache (normalmente bajo Linux) e IIS (Internet Information Server) solo trabaja bajo Windows.**

Otros tipos de servidores incluyen: file servers (servidores para compartir archivos); print servers (servidores de impresión); E-Mail servers; Servers de Negocios online (E-commerce).

**B. Las redes necesitan hardware para conectarse (switches, hubs, routers, modems) y conexiones (cables de red, líneas telefónicas, frame relay, DSL, cable modem, ISDN y otros). Sino los clientes NO pueden conectarse a los servidores.**

En la figura vemos un esquema sobresimplificado de una LAN con conexión a internet.
Por ejemplo la subnet (red) 192.168.57.0 se conecta con 192.168.60.0 a través de un router (Router 1) El router tiene dos interfases (una en cada subnet). Las máquinas de cada subnet están conectadas por un hub o switch.
La conexión a internet la realiza un Router 2.




**C. Los clientes y servidores deben hablar los mismos protocolos de red.**

Las máquinas (sus sistemas operativos) deben hablar el mismo "idioma de red" (network transport protocol)

***Sistemas operativos más usados*: UNIX, Windows, Linux, Novell**

Han existido diversos protocolos de comunicación:
-NetBEUI (Network Basic Input /Output System Extended User Interfase). Un Viejo protocolo de Microsoft /IBM/ Sytex usado para soportar pequeñas redes).
-IPX / SPX (Internet Packet Exchange / Sequenced Packet Exchange) el protocolo que Novell NetWare utilizó durante muchos años.
-TCP / IP (Transmition Control Protocol/ Internet Protocol) el protocolo casi universal utilizado hoy.

Si TCP/IP es nuestro protocolo de comunicación, utilizaremos ciertos servidores fundamentales para soportar su implementación:

-Servidor DNS (Domain Naming System) que conoce los nombres de las computadoras en la red y nos traduce a su numero IP

-Servidor DHCP (Dynamic Host Configuration Protocol) nos ayuda a configurar las maquinas de nuestra red con su configuración IP
-WINS (Windows Internet Name Service) hace algo parecido a DNS pero sobre los nombres Net BIOS de nuestras maquinas. Como NETBIOS es una interfase (API) de la implementación de redes Microsoft WINS NO será necesario en un entorno exclusivo UNIX.

**D. Las redes necesitan seguridad.**

Una vez establecidos los puntos A, B y C el trabajo ha concluido: Puedo leer y escribir archivos en el file server, ver páginas web en el web server, imprimir en impresoras manejadas por el print server…
Pero ésta idea de compartir y de estar ofreciendo los servicios lleva implícita un peligro. Nos está faltando entender cómo me protejo de alguien que quiera aprovechar ésta configuración para hacer un daño o robar información La palabra seguridad aparece junto con dos conceptos fundamentales: autenticación y permisos.
1. Debo autenticar (verificar, identificar) a quien pretenda entrar a mi red y obtener un servicio.
2. Una vez autenticado debo tener almacenado en algún lugar la información de "qué" tiene permitido hacer en la red. (sus permisos).

El punto 1 de seguridad llamado autenticación normalmente se logra con una "cuenta" (nombre de usuario, user id) y un password (contraseña). Hoy existen variantes más sofisticadas: smart cards y tecnologías biométricas (huellas digitales, cara, voz, retina).
Ahora debo guardar la información de usuarios y sus passwords en alguna base de datos centralizada, y necesito "encriptar" esa información. Recordar que siempre existe la posibilidad de que alguien acceda o robe esa base de datos. Por ejemplo los servidores NT4 guardaban información de usuarios en un archivo llamado SAM. Aún cuando el archivo estaba encriptado un grupo de hackers logró saber como crackear la información. Hoy Windows 2000 y 2003, que se basan en dominios, usan un modo más sofisticado de encriptación cuya información también es posible descifrar (el archivo se llama NTDS.DIT en lugar de SAM).

Aclaremos que el peligro está si alguien accede físicamente a esos servidores (domain controlers, DC) donde se guardan las cuentas / passwords. Por eso normalmente esos servidores deberán estar a buen resguardo.

Síntesis: Tenemos un servidor en algún lugar de la red con las cuentas y passwords. Por ejemplo la infraestructura que MS usa para organizar la red se llama Active Directory . Y el servidor con cuentas y passwords (Domain Controler) DC que lo podemos pensar como un servidor de logueo.
Ahora cualquiera que quiera acceder a los "beneficios" de la red se deberá sentar en alguna máquina y entrar user ID y password: logonearse.

Pero ahora surge un problema muy serio. Yo tipeo mi user ID y password y estos deberán viajar por la red para ser verificados en el DC. Pero no existen programas llamados "sniffers" que pueden ver los paquetes que viajan? Sí. Por eso diferentes estrategias han sido y son utilizadas para realizar ésta acción de logonearme para poder acceder a algún recurso de red compartido sin comprometer el password.
Por ejemplo MS utilizó hasta los servidores NT un método de autenticación llamado NTLM (NT LAN MANAGER). Hoy en una red que use Active Directory se usará un viejo método del mundo UNIX (1980) llamado Kerberos. (en NEX 6, Marzo 2004 veremos detalles).
Aparecen hoy otros modos de autenticarse como por ejemplo las llamadas "smart cards". Ellas utilizan una infraestructura diferente llamada PKI (Public Key Infrastructure) basada en certificados y dos claves (keys), una pública y otra privada (en NEX 6; Marzo 2004 veremos detalles).
Aclaremos que hemos ejemplificado el proceso de autenticación al de una persona (usuario). Pero también deberán autenticarse las máquinas entre sí y los servicios. Las infraestructuras detalladas antes también serán usadas en estos casos.

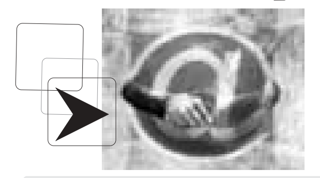
El segundo punto son los Permisos y Access Control Lists (ACLs). Una vez autenticado la pregunta es a qué tiene derecho dentro de la red. Eso se gobierna con una infraestructura de permisos también llamados derechos y privilegios. Ejemplos:

-El file server de la empresa tiene 6 carpetas compartidas pero el usuario "Pepe"solo puede acceder (tiene permiso) para una sola. Y quizás el permiso solo lo deje "read" (leer) los archivo pero no modificarlos
-El usuario "administrador" tiene derecho a crear cuentas de usuarios

Con lo anterior (autenticación y permisos) ejemplificamos uno de los temas que componen la seguridad en el mundo IT. Pero no son los únicos. Por ejemplo
- Cuando solicito información a un website o envío/recibo un e-mail, cómo puedo hacer para que nadie vea los contenidos? La respuesta es encriptándola
- Como me aseguro de quien me envía un cierto e-mail?. Respuesta: digital signing.
- Como hago una compra segura con mi tarjeta de crédito via web?. Normalmente aparece https y no http en el browser. La comunicación a partir de ahí se hará encriptada usando SSL (Secure Sockets Layer) que utiliza encriptación asimétrica de llaves publica y privada (PKI).
- Porque un hacker puede acceder a mi computadora utilizando las llamadas "vulnerabilidades"?
- Que significa que el programa .exe que llega como attachment en un e-mail me cree un back-door?
Todos estos y otros conceptos que conforman la seguridad informatica (ingeniería social, hashes, virus, gusanos, troyano...) también serán expuestas en sucesivos números de NEX.

**E. Las redes deben proveer modos para que los usuarios encuentren los servicios (servidores y recursos compartidos (shares))**

Hace no mucho tiempo utilizar web servers no era tan común y básicamente file y print sharing eran las dos funcionalidades más comunes de las redes. Estas dos acciones siguen siendo importantes solo que los file servers y print servers en la red, pueden ser muchísimos. La pregunta es cómo hago para encontrar un recurso compartido en mi red? Por ejemplo la respuesta de MS en W2000 y W2003 ha sido: Active Directory. Pero ésta tecnología está aún en proceso. Hoy lo más utilizado es una vieja tecnología conocida por "Network Neighborhood o en W2000 y 2003 "My Network Places" que utilizan toda una infraestructura de "browse masters" y "browser lists".



## Windows Services para Unix (SFU) (Mejorado y GRATIS!!)

**SFU permite a los clientes utilizar varias opciones de interoperabilidad, como autenticar usuarios de UNIX y Linux en contra de Active Directory (AD); compartir recursos a través de todas las plataformas con un manejo apropiado de los privilegios de usuario, permitiendo correr aplicaciones UNIX en Windows.**

Microsoft presentó la última versión de su herramienta Windows SFU versión 3.5, la cual tiene como característica varias reformas técnicas importantes. Lo mas impresionante de esta versión es su costo. Por primera vez, Microsoft está entregando licencias SFU gratuitamente a sus clientes de Windows. Así otro producto que previamente se comercializaba por separado es incluido dentro del producto Windows, así como en el caso de Microsoft Internet Explorer (IE) ó Windows Media technologies. No es claro si esta combinación es el resultado de la competencia con Linux. Si, que será un beneficio para cualquier corporación que quiera migrar sus aplicaciones Unix a Windows o mejor aún para quienes integren Windows, UNIX y Linux en un ambiente heterogéneo.

El SFU es una herramienta de interoperabilidad diseñada para integrar varias versiones de Windows (Windows Server 2003, Windows XP, Windows 2000 Server y Win2k Professional) (Windows NT 4.0 no está soportado en esta edición) con UNIX y cada vez más, Linux. SFU incluye un entorno runtime para aplicaciones UNIX basada en tecnología y scripts de Interop Systems y que deja correr aplicaciones UNIX, en máquinas de Windows y soporta tecnologías UNIX tal como NFS y Network Information Service (NIS). "Pocos de nuestros clientes tienen entornos Windows puros" dijo Oldroy (director Windows Server Group en Microsoft). "

En vez de esto tienen una mezcla de Windows, UNIX y Linux. En éstas empresas, la interoperabilidad es tan importante; (las empresas) quieren tener servicios de directorio y servidores de archivos a través de estas plataformas, y lo quieren hacer sin tener que comprar nuevo software".

SFU permite a los clientes utilizar varias opciones de interoperabilidad, como autenticar usuarios de UNIX y Linux en contra de Active Directory (AD); compartir recursos a través de todas las plataformas con un manejo apropiado de los privilegios de usuario, permitiendo correr aplicaciones UNIX en Windows.

También provee herramientas familiares con las cuales cuentan los desarrolladores de UNIX, profesionales IT y administradores: se encontrará con shells C y Korn, aplicaciones y comandos tales como gcc, make, emacs, vi, sendmail y ftp. SFU también incluye Perl 5.6.1 y ActivePerl de ActiveState con esto puede simplificar la migración de los scripts de administración UNIX a Windows.

Cuando usted necesita mover aplicaciones UNIX a una plataforma más accesible, la opción obviamente es Linux. Sin embargo, Microsoft sostiene que SFU en Windows es la solución más barata. Usted tiene que basar cualquier estimación de costo en la experiencia de su empresa con varios sistemas operativos. Pero con el movimiento a una licencia libre en SFU 3.5, Microsoft está terminando con una de las permanentes quejas. Aunque la versión anterior fue vendida por U$s 99 a cada cliente o servidor, SFU es ahora discutiblemente tan barata (o más barata) como una solución Linux.

Entonces, ¿qué es lo nuevo en SFU 3.5? "Esta versión es una actualización de SFU 3.0 (publicado en Mayo del 2002)", dijo Oldroyd. "Tiene el mismo núcleo de funcionalidad pero está mejorado con nuevas características.

Todavía es la migración más completa que existe, y está soportada y patrocinada por Microsoft, lo que muchos de los clientes han estado reclamando. Ellos nos dijeron que entreguemos esta funcionalidad para que ellos puedan evaluar su inversión en su Windows back end." Específicamente, SFU 3.5 incluye rediseños para herramientas de interoperabilidad NFS, NIS y medios Interix; soporte para aplicaciones UNIX P-Thread, permitiendo así migrar aplicaciones multi-threaded (algo que no era posible previamente); mejor soporte POSIX; las últimas versiones de X11 (X11R.6) y muchos utilidades UNIX command-line.

La primera versión en soportar Windows 2003 es SFU 3.5, el cual es más escalable que versiones antiguas y es cluster aware para una mejor disponibilidad.
También soporta características nativas de Windows 2003 tales como Volume Shadow Copy Service (VSS), suministrando copias de recursos compartidos point-in-time y backup y posibilidades de recuperación.

El SFU 3.5 se instala fácilmente. El set de instalación por defecto es diferente para sistemas operativos clientes y servidores.

Las predicciones son que el SFU 3.5 motivará compañías que se hayan estandarizado en infraestructura Windows pero que siguen manteniendo sistemas UNIX. Esas compañías, que todavía utilizan sus más importantes servicios en sistemas UNIX, se dividirán con igualdad entre Windows y Linux, dependiendo de sus necesidades. De cualquier manera el SFU3.5 es un "killer deal" y es un producto que debe evaluar si tiene que migrar UNIX o necesidades de interoperabilidad.

Se puede bajar SFU 3.5 desde el sitio web de Microsoft (http://www.microsoft.com/windows/sfu)

## Un RAM Tester Gratis para Microsoft

La supuesta inestabilidad de muchos sistemas Operativos Windows en muchas casos puede provenir de un problema con la RAM (módulos de memoria mal emparejadas, sobrecalentamiento de sistemas de memoria con ventiladores defectuosos o inadecuados, o sistemas con fuentes eléctricas defectuosas (nótese que los dos últimos no son realmente problemas de memoria. Son muy difíciles de detectar parececiendo "verdaderas" fallas de RAM).

Existe un gran número de RAM testers económicos pero no muy buenos. Los buenos son caros. Ahora, sin embargo, Microsoft está regalando un programa RAM tester.

Se puede encontrar en http://oca.microsoft.com/en/windiag.asp -- un URL que probablemente reconozca. oca.microsoft.com viene de "análisis crash online". Si usted ha tenido una "blue screen" en un sistema XP, entonces recordará que un mensaje ofrece analizarlo por usted - es oca.microsoft.com que contiene el código que hace esto.

El RAM tester parece muy exhaustivo y le resolverá sin duda problemas de RAM.

# ISA Server

**El enorme avance de Internet en el desarrollo de los negocios ha generado la necesidad de disponer de los recursos de IT donde sea que los trabajadores de la información se encuentren realizando sus tareas: trabajadores remotos, socios de negocios y clientes necesitan acceso a servidores internos para correo electrónico, planificación de actividades, páginas Web, carga y descarga de archivos y más. Proveer ese tipo de acceso, sin embargo, potencialmente puede acarrear riesgos en la seguridad de nuestra infraestructura de sistemas..**

**Application-Layer Filtering**

## Introducción a Microsoft Internet Security and Acceleration Server

Primera Parte

A principios de la década del 90, era evidente que Internet iba a convertirse en un recurso indispensable para el desarrollo de los negocios. En esta etapa, la infraestructura necesaria para la provisión de servicios básicos como el correo electrónico y soporte de páginas Web era provista por terceras partes léase Hosting- debido principalmente a dos razones: la primera, el alto costo de los enlaces de acceso a Internet y de su hardware asociado y en segundo lugar, la muy alta demanda de administración y soporte que el software asociado necesitaba por su intrínseca inestabilidad y poca escalabilidad. Esta demanda de servicios dio lugar al desarrollo de grandes compañías dedicadas exclusivamente a soportar la creciente demanda de este tipo de servicios.

Desde el punto de vista de la administración de los servicios internos de IT en las empresas, la conexión hacia los proveedores de servicio era realizada por demanda: es decir, en el momento en que era requerido acceder al correo electrónico o actualizar una de páginas Web de la empresa, se creaba una conexión directa hacia la red de nuestro *Hoster* (generalmente se accedía vía MODEM a través de la red telefónica) y a continuación se descargaban los correos electrónicos o se actualizaba la información de nuestras páginas; una vez finalizada la conexión, nuestra red quedaba aislada del mundo exterior.

Desde el punto de vista de la seguridad, este esquema de conexión/desconexión *on demand* implicaba por defecto poco riesgo de exposición a ataques remotos: una correcta implementación de un sistema anti-virus era generalmente suficiente para mantenernos a salvo de agresiones externas.

A mediados de la década pasada, la situación cambió dramáticamente. La baja en los costos de acceso a Internet, la robustez y facilidad de acceso a la electrónica necesaria para ello y principalmente la evolución del software (conjuntamente con una drástica disminución de su valor) en confiabilidad, disponibilidad y escalabilidad han posibilitado a los administradores de IT tener las herramientas necesarias para soportar internamente todos los servicios de Internet que el negocio demande.

La realidad nos indica que la mayoría de las compañías necesitan estar *conectadas permanentemente* a Internet: nuevas formas de comunicación en los negocios (como la mensajería instantánea), el altísimo volumen de correo electrónico enviado y recibido diariamente, la aparición de Web Services son algunos ejemplos que hacen innegable esta realidad.

Open Systems Interconnection (OSI) Reference Model

Figura 1 -Payload

### Firewalls

Desde el punto de vista de la seguridad, estar *on line* generó nuevos requerimientos a los administradores de IT. Usuarios maliciosos o aún la competencia disponían ahora de un punto *permanente* de ataque: esta situación derivó en la necesidad de *inspeccionar cada paquete (unidad de información) enviado o recibido hacia o desde Internet.*

La aparición en escena de los Firewalls vino a cubrir esa creciente necesidad de monitoreo de información. Los firewalls tradicionales inspeccionan los paquetes a niveles de *transport y network (ver fig. 1), examinando el header (encabezado; ver fig. 2) y tomando la decisión de permitirle el ingreso a la intranet en función de la dirección Internet que envió el paquete, la dirección interna a la cuál ha sido enviado, el tipo de protocolo (TCP/UDP) y sus respectivos números de puertos.*



### El misterio de DNS: "Funciona para la mayoría de los sitios, pero no en Yahoo ni Microsoft.."

Ahora que el mundo está más familiarizado con los firewalls (debido a la creciente actividad de criminales cibernéticos) y con el DNS (Domain Name Server) (debido al creciente uso de Active Directory) muchas veces surge la siguiente pregunta que está ligada a DNS:

"Los encargados de la red han estado haciendo algo recientemente y ahora el DNS no debe estar funcionando bien. Podemos analizar sitios como www.lanacion.com.ar y muchos otros, pero no podemos entrar en Yahoo, Microsoft y algunos otros. ¿Qué puede ser esto?"

La respuesta es que la gente de sistemas abrieron el puerto UDP 53 para DNS, pero no el puerto TCP 53.

DNS casi siempre usa el puerto 53 con UPD (debido a la velocidad de este). Pero fíjense que dije "casi" ya que a veces usa TCP. Cuál utiliza está condicionado por el tamaño máximo del datagrama. (DNS usa puerto 53 como fuente y destino, al contrario de otros protocolos en donde uno le "habla" al server en un puerto y este le responde en un puerto de número más alto. Por ejemplo, si uno quiere ver una página web, interroga el web server en el puerto 80 y este responderá con algún puerto numerado por encima de 1023 (llamado "high port").

Ahora, cuando se consulta una web page, indirectamente consultamos al DNS diciendo "¿cuál es la dirección IP de www.lanacion.com.ar?". En este caso obtendrá solamente una dirección IP (una pequeña respuesta) que cabe dentro de UDP sin ningún problema. Pero trate de hacer esto con sitios como www.yahoo.com ó www.microsoft.com que tienen más de un número de direcciones IP asociados con sus nombres. El DNS no puede poner la respuesta completa dentro del paquete UDP, entonces el DNS cambia al TCP.

Ahora, para el 99.9% de los sitios web se devuelven no más de uno o dos direcciones IP, y por esto son candidatas para UDP. Por esta razón, la gente que configura los firewall probablemente abre sólo UDP port 53 y testea con una cantidad de DNS lookups, con éxito. Pero si dejan cerrado el TCP port 53 , luego verán que de vez en cuando falla del DNS. La respuesta a esto es abrir el TCP port 53.

Esto también puede afectar a la transferencia de zonas, las cuales son generalmente lo suficientemente grandes para necesitar una conexión TCP.

**La Evolución de la Especie**
En este estado de situación, los firewalls tradicionales son tan efectivos que movilizaron a los creadores de software malicioso (Worms, Back Doors tools, denial of service attacks) a escalar en la complejidad de sus ataques llevándolos a la cima del stack: application layer (ver fig. 1).

En este punto, ya no es posible confiar en que el paquete de información examinado tiene lo que su encabezado *dice* contener. Un claro ejemplo de esta evolución es el troyano Back Orifice, originalmente concebido para comunicarse con su controlante a través del puerto 31337 del protocolo TCP. Esta particularidad hacía que el tráfico por él generado fuera fácilmente detectado y por consiguiente bloqueado.

Las más recientes versiones del Back Orifice pueden utilizar cualquier puerto, incluyendo el puerto 80 (http, tráfico Web), haciendo virtualmente imposible a los firewalls tradicionales detectarlo ¿cómo podría uno de estos dispositivos diferenciar el tráfico malicioso




Figura 2 -Payload

generado fuera fácilmente detectado y por consiguiente bloqueado. Las más recientes versiones del Back Orifice pueden utilizar cualquier puerto, incluyendo el puerto 80 (http, tráfico Web), haciendo virtualmente imposible a los firewalls tradicionales detectarlo ¿cómo podría uno de estos dispositivos diferenciar el tráfico malicioso generado por uno de estos troyanos del legítimo tráfico Web? La respuesta es inspeccionando el *contenido* de los paquetes, lo que sería su carga útil o *payload* (ver fig. 2).

Estos firewalls poseen la inteligencia necesaria para tomar decisiones basadas en los datos dentro de los paquetes (payload) en lugar de sólo la información contenida en el header.

No podemos dejar de mencionar que la sobreutilización del puerto 80 del TCP también ha contribuido a la necesidad de poseer un mayor nivel de discernimiento a nivel de la capa 7 o *application layer* (ver fig. 1). Ejemplo de utilización de dicho puerto son las aplicaciones de mensajería instantánea, OWA (Outlook Web Access) y XML Web Services entre otros.

Por último, debemos lamentablemente considerar uno de los factores de mayor demanda de administración: el SPAM. El increíble y por demás preocupante incremento de correo electrónico basura ha posicionado sin lugar a duda a los firewalls como la primera línea de defensa contra este tipo de invasión.
Los altísimos costos derivados de soportar una infraestructura de IT (mayor ancho de banda de acceso a Internet y principalmente la estructura de servidores de mensajería) diseñada para recibir una cantidad inverosímil de correo electrónico que no solo no favorece el desarrollo del negocio, sino que por el contrario disminuye notablemente la productividad de los usuarios que a diario deben desperdiciar valioso tiempo de trabajo en seleccionar el correo útil del que no lo es, urge a los responsables de IT a implementar una solución de filtrado que evite que ese tipo de mensajes alcance siquiera a los servidores de correo: si diseña e implementa una solución apropiada de *firewall filtering* le aseguro que su administrador de Exchange estará infinitamente agradecido.

**Microsoft ISA Server 2000**
Internet Security and Acceleration Server 2000 (ISA Server 2000) es la respuesta de Microsoft a esta creciente demanda de *application-layer filtering*, y aún más. Si bien ISA Server posee todas las características de los firewalls tradionales, ha sido optimizado para applicationlayer filtering. Su arquitectura extensible (ver fig. 3) diferencia notoriamente a este producto de los demás firewalls del mercado.

Este diseño flexible -en conjunción con el SDK (*Software Development Kit*) del producto provisto por Microsoft- posibilita a terceras partes crear sus propios filtros (ver fig. 3),



Figura 3 -Arquitectura Modular de ISA Server

extendiendo de este modo la funcionalidad del producto en relación a la evolución de las formas de ataque o invasión, como así también a nuevas necesidades del negocio.

Desde el punto de vista de la seguridad, la capacidad de *application-layer inspection* posibilita que el producto pueda ser utilizado como *application gateway*: ISA Server 2000 recibe todos los paquetes destinados a la intranet, los analiza, y de ser procedentes realiza una petición equivalente al servidor interno correspondiente en *nombre* del cliente externo. Luego, ISA recibe la respuesta del servidor, reempaqueta la información y la envía al cliente. Esta característica no es menor, pues posibilita que el firewall se comporte como un verdadero intermediario para todo el tráfico, y asegura que no haya tráfico inseguro de Internet enrutado directamente a la red interna.

Desde la óptica del rendimiento, examinar cada uno de los paquetes que llegan desde Internet conlleva la consecuente penalidad de performance, lo cual es resuelto eficientemente a través de la capacidad de escalibilidad del producto Network Load Balancing e ISA Arrays- y con *reverse caching* el contenido interno frecuentemente requerido es alojado en la RAM del servidor ISA y desde allí enviado a los clientes externos sin necesidad de acceder ante cada petición a los servidores internos-.

En sucesivas presentaciones iremos desarrollando algunas de las configuraciones clásicas de ISA Server 2000, entre las que podemos mencionar ISA Arrays, Network Load Balancing, Web Caching, DMZs, VPNs, Web Publishing, SMTP Publishing, Outlook Web Access y Exchange Server Publishing.

**Conclusión**
Application-layer filtering es una poderosa herramienta para el combate de ataques; una profunda inspección del contenido de los paquetes es un requerimiento imprescindible para la seguridad de las redes hoy en día. Ya no es posible confiar que los protocolos y los puertos de acceso indican las reales intenciones de los usuarios externos. Un firewall como ISA Server 2000 es necesario para detener ataques a nivel de *application layer* antes de que ingresen a la red interna y su flexible diseño permite la instalación de nuevos filtros de contenido a medida de las necesidades del negocio.

Javier Pierini
MCSA/MCSE/MCDBA/MCT

# Suplemento Seguridad

Microsoft®



## Guía de Certificaciones de Seguridad

**Hace poco menos de 2 años, los profesionales de IT (Information Technology), que estuvieran interesados en certificarse en seguridad, tenían pocas opciones para elegir. Desde ese entonces, diferentes vendors (de Hardware y de Software) y entidades independientes, han ideado e implementado certificaciones relacionadas con la seguridad.**

### (ISC)² - El Peso de la Experiencia

(ISC)² (CISSP) (SSCP)

El (ISC)² [Internacional Information Systems Security Certification Consortium] se formó en 1989 con el objetivo de crear un estándar para las prácticas correctas de seguridad en la información. El (ISC)² ha creado varias certificaciones, que no dependen de ningún vendor específico, que combinan los conocimientos, la experiencia, la ética y la educación continua de los candidatos. Una de las certificaciones es: CISSP (Certified Information Systems Security Professional) se enfoca en 10 temas específicos:

- Metodología y Sistemas de Control de Acceso
- Desarrollo de Aplicaciones y Sistemas
- Planeamiento de Continuidad de Negocios
- Criptografía
- Leyes, Investigación y Ética
- Seguridad en Operaciones
- Seguridad Física
- Modelos y Arquitecturas de Seguridad
- Prácticas de Administración de Seguridad
- Seguridad en Telecomunicaciones, Red e Internet

La suma de estos temas, da como resultado un examen de 250 (doscientas cincuenta) preguntas y 6 (seis) horas de duración, aunque, con el simple hecho de aprobar el examen, Ud no obtiene la CISSP. Debido a que (ISC)² exige que los candidatos tengan una experiencia directa full-time con productos de seguridad durante un mínimo 4 (cuatro) años, esta experiencia debe ser documentada por un tercero.
Otra opción, para los que no tienen 4 (cuatro) años de experiencia, es obtener el título SSCP (Systems Security Certified Practitioner). Este examen de 3 (tres) horas y 125 (ciento veinticinco) preguntas solamente abarca 7 de los temas mencionados para la certificación CISSP.
Para ambas certificaciones, el candidato debe firmar y acatar el código de ética de la (ISC)² y completar unidades continuas de educación para mantener los títulos.
La tercer opción es convertirse en Asociado de la (ISC)², de esta manera se pueden rendir primero los exámenes y adquirir luego la experiencia exigida por (ISC)². El costo de los exámenes ronda entre los US$ 450 y US$ 650. Para más información, visite: www.isc2.org.

### SANS Institute - Con el foco en la práctica



GIAC

Así como con el (ISC)², las certificaciones del SANS Institute, no dependen de ningún vendor específico, pero su enfoque es meramente La variedad de certificaciones, giran en torno a la GIAC (Global Information Assurance Certification), las más importantes son:

- GSEC: GIAC Security Essentials Certification.
- GCFW: GIAC Certified Firewall Analyst (*1)
- GSLC: GIAC Certified Security Leadership
- GCIA: GIAC Certified Intrusion Analyst (*1)
- GCIH: GIAC Certified Incident Handler (*1)
- GCWN: GIAC Certified Windows Security Administrator (*1)
- GCUX: GIAC Certified Unix Security Administrator (*1)
- GISO: GIAC Information Security Officer
- GSNA: GIAC Systems and Network Auditor
- GCFA: GIAC Certified Forensic Analyst
- GSAE: GIAC Security Audit Essentials

Aquellos que obtengan las certificaciones marcadas con (*1) pueden obtener la más alta certificación del SANS Institute: la GIAC Security Engenieer. Hasta el momento sólo 2 (dos) personas en el mundo la tienen.
Los exámenes GIAC pueden rendirse on-line ó en las conferencias de SANS y su costo oscila entre los US$ 250 y US$ 450 dependiendo si se toma el entrenamiento (cursos) en el SANS Institute.
Los profesionales certificados GIAC deben re-certificar cada 2 (dos) años, el costo de la re-certificación es de US$ 120. Para más información, visite: www.sans.org y www.giac.org.

### Microsoft - Asegurando Windows

Microsoft

Microsoft debuta con 2 (dos) nuevas certificaciones relacionadas con la seguridad: MCSA Security y MCSE Security. Si Ud. es un profesional en Redes Microsoft, ya no necesita buscar certificaciones de seguridad fuera del ambiente Microsoft.
Estas nuevas certificaciones son directamente análogas a las ya existentes, la diferencia radica en la elección de los exámenes electivos de cada una de ellas, que deben incluir, para cada caso:

- ***MCSA Security 2000:***
  - 70-214 Implementación y Administración de Seguridad en una red Windows 2000
  - 70-227 Instalación, Configuración y Administración de MS-ISA Server 2000, Enterprise Edition ó CompTIA Security+
- ***MCSE Security 2000***
  - Idem MCSA Security 2000
  - 70-220 Diseño de Seguridad en una red Windows 2000.
- ***MCSA Security 2003***
  - 70-299 Implementación y Administración de Seguridad en una red Windows Server 2003
  - 70-227 Instalación, Configuración y Administración de MS-ISA Server 2000, Enterprise Edition ó CompTIA Security +
- ***MCSE Security 2003***
  - Idem MCSA Security 2003
  - 70-298 Diseño de Seguridad en una red Windows Server 2003

En el caso que Ud. ya esté certificado MCSA (Microsoft Certified Systems Administrator) ó MCSE (Micro tienen un costo de US$ 80 (en Latinoamérica) y esoft Certified Systems Engenieer), sólo deberá rendir éstos exámenes para agregar éstos nuevos títulos a su haber.
Los exámenes Microsoftstán disponibles a través de Pearson-VUE y/ó Prometric. Para más información, visite: www.microsoft.com/mcp.

### CompTIA - Seguridad al alcance de todos.

CompTIA.

CompTIA (Computing Technology Industry Association) es conocida por sus Certificaciones de nivel básico y que no son específicas de ningún vendor, por ejemplo: A+, Network+ y Linux+.



Siguiendo esta línea, existe ahora la certificación Security+. Esta relativamente nueva certificación consta de un único examen de 100 (cien) preguntas y una duración de 90 (noventa) minutos, abarcando los siguientes temas:

- Seguridad en Comunicaciones
- Seguridad en la infraestructura
- Criptografía
- Control de Acceso
- Autenticación
- Ataques Externos
- Seguridad en las Operaciones

Es recomendable que quien desee obtener esta certificación tenga un mínimo de 2 (dos) años de experiencia en generalidad de redes. Muchos programas de Certificación aceptan ó recomiendan a Security+ como requisito, por ejemplo MCSA Security ó MCSE Security.
El examen Security+ tiene un costo de US$ 225 y no es necesario renovarlo. Para más información, visite:
www.comptia.org/certification/security/default.asp

### Cisco - Seguridad desde el Hardware



La CCSP (Cisco Certified Security Professional) es una certificación con el mismo nivel de exigencia que la CCNP (Cisco Certified Network Professional) ó CCDP (Cisco Certified Design Professional). Para obtener la CCSP, los candidatos deben obtener (o ya poseer) la CCNA (Cisco Certified Network Associate) ó CCIP (Cisco Certified Internetworking Professional) y además rendir los siguientes exámenes:

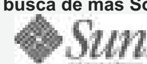
- 642-501 SECUR: Securing Cisco IOS Networks
- 642-511 CSVPN: Cisco Secure VPN (*1)
- 642-521 CSPFA: Cisco Secure PIX Firewall Advanced (*2)
- 643-531 CSIDS (beta): Cisco Secure Indtrusion Detection System (*3)
- 642-541 CSI: Cisco SAFE Implementation

Ahora, si lo que está buscando es una especialización para su CCNA, puede optar por los siguientes:

- Cisco Firewall Specialist (642-501 + (*2) )
- Cisco IDS Specialist (642-501 + (*3) )
- Cisco VPN Specialist (642-501 + (*1) )

Todos éstos exámenes están disponibles a través de Pearson-VUE y/ó Prometric y tienen un costo de US$ 125 (salvo el beta que es de US$ 50). Todas las certificaciones de Cisco requieren una revalidación (ó recertificación) cada 2 a 3 años.
Para los candidatos altamente experimentados existe la certificación CCIE (Cisco Certified Internetwork Engineer). Esta certificación está diseñada para Profesionales de elite y por esta razón no puede obtenerse mediante los métodos tradicionales de estudio y examinación. Los candidatos deben pasar primero un examen de calificación, con un costo de US$ 300 (disponible a través de Pearson-VUE y/ó Prometric) y luego viajar a uno de los 5 laboratorios disponibles en el mundo para rendir el examen CCIE. Este último tiene un costo de US$ 1250 (el costo del viaje no está incluido).
Para más información sobre las certificaciones Cisco, visite: www.cisco.com/en/US/learning/

### Sun - En busca de más Sol



Para dar más variedad a la gama de certificaciones existentes para Solaris, Sun agrega una nueva certificación, esta vez, específica sobre seguridad: SCSA (Sun Certified Security Administrator) for Solaris 9 OS. Los objetivos de este examen incluyen:

- Conceptos Generales de Seguridad
- Detección y Administración de Dispositivos




Suplemento Seguridad

- Ataques a la Seguridad
- Protección de Archivos y Recursos del Sistema
- Prevención sobre la Red y el Host
- Autenticación y encriptación en conexiones de Red

El examen consta de 60 (sesenta) preguntas, con una duración de 90 (noventa) minutos y un costo de US$ 150 y puede rendirse a través de Prometric.
Sun recomienda que los candidatos obtengan previamente la SCNA (Sun Certified Network Administrator) ó la SCSA (Sun Certified System Administrator).
Para más información, visite: suned.sun.com/US/catalog/courses/CX-310-301.html.

## EC-Council - Conocer al enemigo



¿Qué es exactamente un Ethical Hacker? Puesto en palabras sencillas: es la persona que tiene los conocimientos y herramientas necesarias para (intentar) atacar una computadora o una red de computadoras, poniendo a prueba la seguridad de las mismas. Las características que lo diferencian de un Hacker (común) son:
- está empleado por una compañía, para tomar la actitud de un Hacker
- está autorizado por la compañía a realizar estas tareas

La certificación "Ethical Hacker" del EC-Council, consta de un único examen de 50 (cincuenta) preguntas, que entre sus temas incluye: footprinting, hackeo de servidores web, técnicas de crackeo de contraseñas; y está enfocado para los administradores de Sistemas/Redes. El costo del examen es de US$ 125 y puede rendirse únicamente a través de Prometric.
Para más información, visite: www.eccouncil.org/CEH.htm.

## ISecOM - La Metodolog a "Open"

ISecOM (Institute for Security and Open Methodologies) es una organización enfocada sobre una comunidad de colaboradores voluntarios, que tiene por objetivo definir estándares en testeos de seguridad e integridad de negocios, proveer métodos y mediciones preactivos en seguridad e integridad. Este conjunto de métodos se engloban en el OSSTMM (Open Source Security Testing Methodology Manual), convirtiéndose en el principal material de estudio para las certificaciones.
La certificación OPSA (OSSTMM Professional Security Analyst) tiene por objetivo certificar que un profesional puede tomar decisiones prácticas e ingeniosas para solucionar problemas imprevistos de seguridad, basándose en la interpretación de los resultados de testeos, sabiendo como y donde se obtuvieron y lo que significan.
La certificación OPST (OSSTMM Professional Security Tester) tiene por objetivo certificar los conocimientos de un profesional en las herramientas y métodos de testeos de seguridad, tanto para intrusiones desde el exterior como para verificaciones entre la DMZ (De-Militarized Zone) y la red Interna; y vIceversa.
Cada una de estas certificaciones se obtiene rindiendo un examen a libro abierto y laboratorio, de 50 (cincuenta) preguntas y 4 (cuatro) horas de duración, abarcando los siguientes temas:
- Profesionalidad Consultoría, ética y planeamiento de proyectos.
- Enumeración Envío y recepción de distintos tipos de paquetes.
- Estimación Basada en análisis exhaustivo de documentos y resultados de tests.
- Aplicación Investigación y testeo de nuevas aplicaciones de Internet
- Verificación Determinación de servicios y sus vulnerabilidades por medio del testeo.

La certificación OSPE (OSSTMM Professional Security Expert) solamente tiene por objetivo certificar los conocimientos contenidos en el OSSTMM, y a diferencia de las certificaciones OPSA y OPST, el examen no es a libro abierto y consta de 100 (cien) preguntas y 4 (cuatro) horas de duración.
Para más información, visite: www.isecom.org

## Pregunta Microsoft 70-294

### "Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure" (70-294)

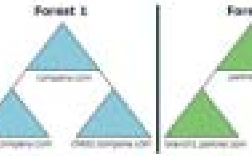
Usted es Administrador de Redes en un "forest" (forest=bosque) de Active Directory llamado **company.com**. La red de un socio de negocios consiste de otro "forest" llamado **partner.com**. Los "forests" están representados en el siguiente esquema: (ver más debajo)

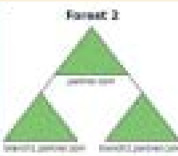
El sistema operativo en ambos "forests" es Windows Server 2003. Los usuarios del dominio **child1.company.com** en su "forest" necesitan acceder a recursos del dominio **branch2.partner.com**. Los administradores del "forest" de su socio deberían ser capaces de asignar permisos a recursos en **branch2.partner.com** sólo a usuarios de **child1.company.com**.

Los administradores de su "forest" no deberían ser capaces de asignar permisos en sus dominios a usuarios del "forest" de su socio. En colaboración con un administrador del "forest" **partner.com**, usted debe configurar la relación de confianza (trust relationship) apropiada.

¿Cuál o cuáles de las siguientes son las características de la relación de confianza que usted debe crear? (Seleccione todas las opciones que crea correctas)

a. Forest
b. Externa
c. Entrante
d. Saliente
e. Transitiva
f. No-transitiva



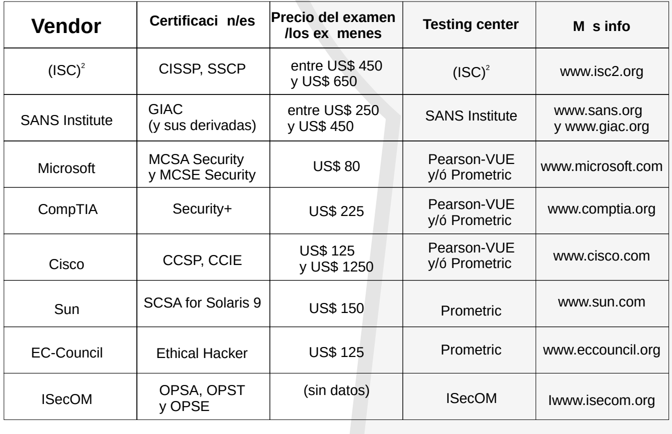




Respuesta:

Sólo las respuestas **b**, **c** y **f** son correctas. Los atributos principales de las relaciones de confianza que pueden ser establecidas en un "forest" de Windows Server 2003 son tipo, dirección y transitividad. Una relación de confianza tipo "forest" es una relación entre todos los dominios en un "forest" y todos los dominios en otro "forest". Las relaciones "forest" se mantienen sólo entre los forests cuyo "functional level" sea Windows 2003. Una confianza externa es una confianza entre un dominio en un forest y otro dominio fuera de ese forest. El segundo dominio puede pertenecer a otro "forest" o puede ser un dominio de Windows NT. La dirección de una relación de confianza es desde los "resources" hacia "security principals". La transitividad significa que dos o más relaciones de confianza separadas pueden ser encadenadas. Si un dominio confía transitivamente en otro dominio y ese dominio lo hace con un tercer dominio, entonces el primer dominio confía en el tercero.

En este escenario, usted debería crear una relación de confianza entrante externa en el dominio **child1.company.com** con el dominio **branch2.partner.com**. Por definición, las relaciones de confianza externas no son transitivas, y las relaciones de confianza "forest" sí son transitivas. Si usted creó una relación de confianza "forest", entonces cada dominio de su "forest" tendrá relaciones de confianza con cada dominio del "forest" de su socio.

Entonces, las cuentas de usuario en dominios confiables se volverían visibles en dominios con los que establezcamos relaciones de confianza; por consecuencia, los administradores en los dominios con los que establezcamos relaciones de confianza serían capaces de asignar permisos para recursos en sus respectivos dominios para usuarios de dominios confiables.



| Vendor | Certificaci n/es | Precio del examen /los ex menes | Testing center | M s info |
|---|---|---|---|---|
| (ISC)² | CISSP, SSCP | entre US$ 450 y US$ 650 | (ISC)² | www.isc2.org |
| SANS Institute | GIAC (y sus derivadas) | entre US$ 250 y US$ 450 | SANS Institute | www.sans.org y www.giac.org |
| Microsoft | MCSA Security y MCSE Security | US$ 80 | Pearson-VUE y/ó Prometric | www.microsoft.com |
| CompTIA | Security+ | US$ 225 | Pearson-VUE y/ó Prometric | www.comptia.org |
| Cisco | CCSP, CCIE | US$ 125 y US$ 1250 | Pearson-VUE y/ó Prometric | www.cisco.com |
| Sun | SCSA for Solaris 9 | US$ 150 | Prometric | www.sun.com |
| EC-Council | Ethical Hacker | US$ 125 | Prometric | www.eccouncil.org |
| ISecOM | OPSA, OPST y OPSE | (sin datos) | ISecOM | Iwww.isecom.org |









# Elementos b sicos de criptograf a

## Parte ½

Definición: la criptografía es la ciencia que nos permite proteger nuestros datos utilizando una transformación matemática de modo de transformarlos en ilegibles.

Un ejemplo:
-cuando necesito enviar/recibir información de un modo seguro a través de una red (intranet, extranet ó internet) la "encriptación" (cifrado) es la herramienta fundamental para poder realizar la tarea.
-si alguien roba mi laptop pero quiero tener un archivo en mi disco rígido que nadie (excepto yo) pueda leer.

¿Qué funciones de seguridad me permite realizar la encriptación ?

Autenticación: permite a quien recibe un mensaje, estar seguro que quien lo envía es quien dice ser.
Confidencialidad: asegura que nadie leyó el mensaje desde que partió. Sólo el destinatario podrá leerlo.
Integridad: asegura que el mensaje no ha sido modificado

Para entender como lograr esto detallaremos tres conceptos básicos de criptografía:

A- Algoritmos hash en un sentido
B- Encriptación con llaves (keys, claves) simétricas: se utiliza una llave
C- Encriptación con llaves públicas y privadas: se utilizan dos llaves

En artículos posteriores desarrollaremos infraestructuras que se construyen sobre éstos. Ejemplos: firma digital o cómo haríamos para intercambiar una llave secreta. Otro ejemplo fundamental es la llamada Public Key Infrastructure (Infraestructura de llave pública) (PKI) que nos detalla las directivas, los estándares y el software que regulan o manipulan los certificados, y las llaves públicas y privadas. En la práctica, PKI hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y otras entidades de registro que comprueban y autentican la validez de cada parte implicada en una transacción electrónica.

Hash

Un hash, también denominado valor hash o síntesis del mensaje, es un tipo de transformación de datos. Un hash es la conversión de determinados datos de cualquier tamaño, en un número de longitud fija no reversible, mediante la aplicación a los datos de una función matemática unidireccional denominada algoritmo hash. La longitud del valor hash resultante puede ser tan grande que las posibilidades de encontrar dos datos determinados que tengan el mismo valor hash son mínimas. Supongamos que quiero "hashear" el siguiente mensaje: "mi mamá". Quiero que el mensaje se resuma en un solo número (valor hash). Podría por ejemplo, asociar a cada carácter ASCII su número (ASCII code number) asociado

"m i <espacio> m a m a"
109 + 105 + 32 + 109 + 97 + 109 + 97 = 658.

Así que el mensaje se "resumió" (digest) en un solo número. Notemos que ésta es una función en una dirección (no reversible). No hay manera de que alguien adivine el mensaje "mi mamá" a partir del 658 a menos que pruebe todos los posibles mensajes (infinitos) ( y calcule sus "valor hash (digest)". Aún así tendría muchísimos con 658 y debería adivinar cuál es el correcto (imposible).

Destacamos que la función (algoritmo) hash usado fue de lo más simple. En la vida real son usados algoritmos mucho más complejos. Podríamos por ejemplo, usar ese número para verificar si un mensaje enviado fue modificado en el camino: el remitente genera con un algoritmo un valor hash del mensaje, lo encripta y envía el hash encriptado junto con el mensaje. A continuación, el destinatario desencripta el hash, produce otro hash a partir del mensaje recibido y compara los dos hashes. Si son iguales, es muy probable que el mensaje se transmitiera intacto. Aquí supusimos que ambos conocen la llave para encriptar/desencriptar.

Funciones comunes de hash en un sentido

Las dos funciones hash siguientes son las más comunes:
MD5. MD5 es un algoritmo hash diseñado por Ron Rivest que produce un valor hash de 128 bits. El diseño de MD5 está optimizado para los procesadores Intel. Los elementos del algoritmo se han visto comprometidos, lo que explica su menor uso.
SHA-1. Al igual que el algoritmo de llaves públicas DSA, Secure Hash Algorithm-1 (SHA-1) fue diseñado por la NSA e incorporado por el NSIT en un FIPS para datos de hash. Produce un valor hash de 160 bits. SHA-1 es un conocido algoritmo hash de un sentido utilizado para crear firmas digitales.

Este artículo continúa en el próximo NEX.






## Certificaciones MCP

| | |
|---|---|
| **MCP** | 965,749 |
| **MCSE** (on Windows 2000) | 228,148 |
| **MCSD** | 44,321 |
| **MCSD** (for Microsoft .NET) | 4,711 |
| **MCDBA** (for SQL Server 2000) | 116,812 |
| **MCSA** (on Windows 2000) | 89,731 |
| **MCAD** (for Microsoft .NET) | 10,522 |
| **MCT** | 11,500 |

Total de Certificaciones: **2.107,406**
fuente: www.mcpmag.com
Datos de Noviembre de 2003
proporcionados por Microsoft corporation

## Pregunta LPI (Linux Professional Institute)

### Examen LPI 101

Mónica consulta el archivo `/etc/passwd` esperando encontrar passwords encriptadas para todos los usuarios de su sistema. Ella ve lo siguiente:

```
jdoe:x:500:500::/home/jdoe:/bin/bash
bsmith:x:501:501::/home/bsmith:/bin/cts
```

¿Cuál de los siguientes es verdadero? Seleccione uno
a. Las cuentas `jdoe` y `bsmith` no tienen contraseña
b. La cuenta `jdoe` y `bsmith` están deshabilitadas
c. Las contraseñas están en `/etc/passwd-`
d. Las contraseñas están en `/etc/shadow`
e. Las contraseñas están en `/etc/shadow-`

Rta correcta: D.

### Examen LPI 102

Ud. tiene un servidor Linux, actuando como *router* a InterNet, todas las PCs de su red interna corresponden a la SubNet `192.168.0.0`, con máscara `255.255.255.0`. Asumiendo que Ud. tiene configurado `iptables`, con su política de `INPUT` establecida en `DROP`, ¿Cuáles de las siguientes reglas de `iptables` permitirán la navegación web? (Marque todas las que correspondan)

a. `iptables -A INPUT -p tcp -d 0.0.0.0/0 --dport 80 -j ACCEPT`
b. `iptables -A INPUT,OUTPUT -p tcp -d 0.0.0.0/0 --dport 80 -j ACCEPT`
c. `iptables -A INPUT -p tcp -d 0.0.0.0/0 --dport 80,443 -s 192.168.0.0/24 -j ACCEPT`
d. `iptables -A OUTPUT -p tcp -d 0.0.0.0/0 --dport 80 -j ACCEPT`
e. `iptables -A OUTPUT -p tcp -d 0.0.0.0/0 --dport 80,443 -s 192.168.0.0/24 -j ACCEPT`
f. `iptables -A INPUT -p tcp -i ppp0 -j ACCEPT`

Rta correcta: C y E.

# SNORT PARA LINUX




**Qué es Snort?**

El Snort es un Sistema de detección de Instrusos (IDS) muy potente, el cual hace las veces de sniffer colocando la interfaz de red de la máquina en la cual se encuentra corriendo en *modo promiscuo, es decir, brinda la capacidad a la placa de red de obtener todos los paquetes que circulan en un mismo hub o switch aún sin ser los suyos.*
El objetivo de Snort es, por sobre todas las cosas, el de alertar en caso de recibir un intento de ingreso o ataque a nuestra red. Para ello se basa en un gran número de reglas que deciden si el evento o paquete recibido corresponde a un ataque o no.
Una de las ventajas más importantes a la hora de optar por Snort como nuestro IDS preferido por sobre los demás, es la gran cantidad de reglas que se encuentran predefinidas hoy en día y el respetable grupo de desarrolladores con el que la organización cuenta, ya que estos últimos son quienes constantemente actualizan dichas reglas.
Una regla se encuentra definida por dos secciones lógicas: Cabecera de la Regla ó "**Rule Header**" **y Opciónes de la Regla ó "Rule Options" donde:**
<u>Cabecera de la Regla</u>:
Contiene la acción, protocolo, puerto e IP/máscara de red Origen y puerto e IP/máscara de red Destino.
<u>Opciónes de la Regla</u>:
Contiene mensajes de alerta e información del sector del paquete donde se debe inspeccionar para determinar si esta se cumple o no.
En el siguiente ejemplo se generará un alerta en caso que alguien intentara conectarse al servidor Telnet local, el mismo arrojará un mensaje con el valor especificado en "msg", lo que permitirá identificar rápidamente el evento en el archivo de log:
**alert tcp any any -> 192.168.1.1/32 23 (content: "pass"; msg: "TELNET!!!!";)**

Es muy importante prestar gran atención a la configuración del mismo, ya que si este se encuentra configurado con una sintaxis errónea podría generar lo que se conoce como "Falsos positivos", es decir, estaría informando alertas falsas, las cuales no harán más que llenar el disco de información innecesaria.

**Como instalarlo?**
Para instalar Snort se deberá bajar el código compreso de su sitio oficial (www.snort.org), en la sección "downloads" se encuentran las versiones disponibles, las mismas pueden bajarse precompiladas (En formato binario) o bien para compilar. Una vez obtenida la versión que más se ajuste a las necesidades se procederá a la instalación:
En caso de haber optado por el paquete rpm:

*rpm Uvh snort-1.9a.rpm*

Este procedimiento es muy sencillo, ya que al instalar el paquete rpm, automáticamente se crean los directorios con las diferentes reglas y el archivo de configuración principal del programa.
En caso de haber optado por el source:

*$ tar zxf snort-2.0.0.tar.gz*
*$ cd /snort-2.0.0*
*$ ./configure*
*$ make*
*$ make install*

Una vez instalado el source se deberá instalar el paquete de reglas actualizadas, el cual incluye el archivo de configuración general, este mismo puede ser obtenido también dentro de la sección "downloads" de la página oficial.

*$ mkdir /etc/snort*
*$ cp snortrules-stable.tar.gz /etc/snort*
*$ tar -zxfv snortrules-stable.tar.gz*
*$ rm snortrules-stable.tar.gz*

Luego se procederá a la edición del archivo de configuración principal mediante cualquier editor de texto:

*$ vi /etc/snort/snort.conf*

Al editarlo se podrá observar gran cantidad de líneas comentadas, las mismas ayudarán a la comprensión de cada una de las opciones a configurar. Las opciones más importantes para configurar son las siguientes:
<u># Definición del rango de direcciones de la red interna:</u>
# Para ello se deberá optar por alguna de las posibilidades descriptas (Solo una)

**var HOME_NET 192.168.0.0/24**
# Define un rango de direcciones de red.
**var HOME_NET $eth0_ADDRESS**
# Define el rango de direcciones de red al cual pertenece la interface de red eth0 al iniciar Snort
**var HOME_NET [192.168.0.0/24,192.168.1.0/24,10.0.0.0/24]**
# Define diversos rangos de direcciones de red.

<u># Definición del rango de direcciones de la red externa:</u>
**var EXTERNAL_NET any**

<u># Definición de direcciones de red de algunos servidores importantes:</u>
**var DNS_SERVERS [192.168.0.1,24.232.0.17,24.132.21.0.18]**
**var SMTP_SERVERS 192.168.0.1**
**var HTTP_SERVERS [192.168.0.2,192.168.1.2]**
**var SQL_SERVERS [192.168.0.1]**

Una vez configuradas las variables más importantes se deberán habilitar los diversos preprocesadores, los cuales se encargaran de analizar los paquetes y detectar intentos de hackeo, ataques, escaneo de puertos, y demás.
El mecanismo a seguir para la activación de los diferentes preprocesadores es la de visualizar los comentarios de cada una de las opciones para reconocer cuales son los que se ajustarán a las necesidades y luego descomentar cada una de las líneas, por ejemplo, para activar la detección de escaneo de puertos se deberá activar el procesador "portscan", para ello habrá que descomentar la siguiente línea:
**preprocessor portscan: 192.168.1.0/24 5 7 /var/log/portscan.log**
La sintaxis afirma que si en 7 segundos se accedieran a 5 puertos distintos, entonces la información quedará reflejada en el archivo de log "portscan.log".

**preprocessor portscan-ignorehosts: 192.168.1.1/32 192.168.0.1/32**
En este caso se estaría ignorando cualquier tipo de scaneo de puertos proveniente de los hosts especificados.

Finalmente, se deberán configurar las salidas (Output) de información, es decir, que tipos de registros generar (utilizando Syslog, archivos de textos propios, registros en una base de datos), donde se alojarán dichas salidas y cual será su formato.
En caso de necesitar reflejar los eventos en el syslog se deberá descomentar la siguiente línea donde se podrá apreciar tanto la facilidad como el argumento del syslog:
**output alert_syslog: LOG_AUTH LOG_ALERT**

Si por el contrario se deseara arrojar la información de los eventos a una base de datos (MySQL) se deberá descomentar la siguiente línea:
**output database: log, mysql, user=snort password=*ppp* dbname=snort host=localhost**

Cabe aclarar que en caso de arrojar la información a una base de datos, previamente se deberán instalar los paquetes necesarios para el funcionamiento del Servidor SQL (Mysql / Postgresql). Además al momento del compilar el snort se deberá parametrizar el soporte para SQL:
**./configure --with-mysql**

La información recolectada por el Servidor de base de datos puede ser consultada por línea de comandos o vía web mediante un soft adicional llamado **ACID, quien se encargará de la visualización de los logs recogidos por Snort, este soft no necesita ningún tipo de instalación, simplemente se deberá bajar el paquete tar.gz del sitio http://acidlab.sourceforge.net/, descompactar el archivo en algún directorio dentro del "DocumentRoot" (Por ejemplo /acid) correspondiente a la configuración del Servidor apache y luego acceder a la interfaz web vía: http://direccion-del-virtualhost/acid/acid_main.php**

En la sección final del archivo de configuración se invocan todas las reglas incluídas dentro del directorio /etc/snort, las mismas contienen definiciones de alertas como la comentada en el ejemplo del comienzo. Para incluir nuevas reglas tan solo hay que agregar una línea al final del archivo con el siguiente formato:

**include $RULE_PATH/regla_nueva.rules**

Martin Sturm
MCSA, MCSE, LPIC (101/102/201)





**El objetivo de Snort es, por sobre todas las cosas, el de alertar en caso de recibir un intento de ingreso o ataque a nuestra red. Para ello se basa en un gran número de reglas que deciden si el evento o paquete recibido corresponde a un ataque o no.**

# Linux, con la lupa en la seguridad

Fuente: www.hispasec.com

A continuación vamos a enumerar una lista de distribuciones Linux que ponen énfasis en las herramientas para aumentar los niveles de seguridad. Es importanteaclarar que todas funcionan como "Live CD" lo que quiere decir que se ejecutan directamente desde el CD, no hace falta instalarlas, esto es particularmente útil en los casos en que lo que necesitamos es una herramienta para revivir el disco o recuperar los datos.
Cómo varias de las distribuciones que presentamos a continuación están basadas en Knoppix, comentaremos que ésta distribución es un CD arrancable con una colección de programas GNU/Linux software, detección automática de hardware, y soporte de muchas tarjetas gráficas, tarjetas de sonido, dispositivos SCSI y USB y otros periféricos. KNOPPIX puede ser usuado como una demo de Linux, CD educacional, sistema de rescate, o adaptado y usado como plataforma comercial de demos de productos. Como ya hemos dicho NO es necesario instalar nada en el disco duro. Debido a la descompresión en-demanda el CD tiene casi 2 GB de programas ejecutables instalados en el.

KNOPPIX.net

**Knoppix STD 0.1b**
STD (Security Tools Distribution) es una versión personalizada de Knoppix. Utiliza el núcleo 2.4.20 y KDE 3.1, da soporte a una gran cantidad de dispositivos de hardware (que son detectados y configurados automáticamente). Cuando se arranca la máquina con Knoppix STD, no se realiza ningún tipo de modificación en la configuración de la computadora.
Todas las herramientas de Knoppix, al igual que toda la distribución, estan diseñadas para ser ejecutadas directamente desde el CD y están dividas en varias categorías: herramientas para la gestión de redes; herramientas para la realización de valoraciones de seguridad y herramientas para la realización de pruebas de redes; un gran número de herramientas para la realización de pruebas de penetración, sniffers; herramientas para el análisis forense, cortafuegos, honeypots, sistemas de detección de intrusiones ; autenticación, identificación de contraseñas y cifrado.
Se puede conocer mas y obtener la distribución en www.knoppix-std.org.

**LocalAreaSecurity 0.4**
Muy pequeña (185 MB), pensada para instalarse en un CD chico, como los tipo tarjeta de crédito). También está basada en Knoppix y utiliza el núcleo 2.4.20. LocalAreaSecurity está pensado para la realización de pruebas de verificación de la seguridad y pruebas de penetración. Para eso cuenta con un gran número de herramientas especializadas: sniffers, cifrado, monitorización de redes, detección de información oculta, obtención de información, etc.
Se puede conocer mas y obtener la distribución en www.localareasecurity.com.

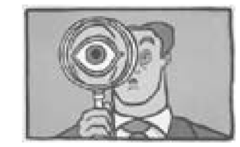
**Phlak (Prof. Hacker's Linux Assault Kit) 0.1**
Basado en Morphix. Viene con dos GUI livianas (fluxbox y XFCE4). Está especializada en la realización de análisis de seguridad, pruebas de penetración, análisis forense y auditorios de seguridad.
Incluye herramientas de análisis de tráfico, de protocolos, de funcionamiento del sistema, de extracción de datos de sistemas de archivos, cifrado de archivos, sniffers, etc.
Se puede conocer mas y obtener la distribución en www.phlak.org.

**R.I.P. (Recovery Is Posible)**
Esta distribución, está pensada para recuperar datos de sistemas de archivos dañados. Funciona con lso sistemas de archivos ext2, ext3, reiser, jfs, xfs, ufs, NTFS, FAT16 y FAT32.
Se puede conocer mas y obtener la distribución en http://www.tux.org/pub/people/kent-robotti/looplinux/rip/.




**WARLINUX 0.5**
Es una distribucón live CD pensada específicamente para identificar las redes inalámbricas que están al alcance y realizar auditorías y verificaciones de los niveles de seguridad de las mismas.
Se puede conocer mas y obtener la distribución en http://sourceforge.limpio/projects/warlinux/.

**F.I.R.E.**
Esta versión de Linux incluye las herramientas necesarias para la realización de valoraciones de seguridad, respuesta a incidentes de seguridad, pruebas de penetración y análisis forense de sistemas y recuperación de datos en sistemas Windows, Solaris (SPARC) y Linux (x86). Adicionalmente, FERIO incluye un programa para la detección de virus (F-Prot).
Se puede conocer mas y obtener la distribución en http://biatchux.dmzs.com.



Existen otras distribuciones similares a estas:

**Penguin Sleuth Kit**
**http://www.linux-forensics.com/downloads.html**

**@stake Pocket Security Toolkit v3.0**
**http://www.atstake.com/research/tools/pst/**

**ThePacketMaster Linux Security Server**
**http://freshmeat.net/projects/tpmsecurityserver/**

**Trinux**
**http://trinux.sourceforge.net/**

Lo anterior evidencia que existe una enorme cantidad de herramientas puestas a nuestra disposición. Lo más interesante de esto es que podemos contar con sistemas operativos completamente funcionales sin necesidad de instalarlos, esto es muy útil, cuando en NO PODEMOS instalarlos justamente debido a que nuestro sistema ha dejado de responder. Aunque debemos destacar que la existencia de éstas herramientas no nos absuelve de la responsabilidad de realizar backups de nuestros datos ni de prestar la debida atención a las configuraciones de seguridad de nuestras redes; el dicho es muy viejo pero sigue siendo cierto y muy aplicable a las Tecnologías de la Información: "mejor prevenir que curar".



# Ethical Hacking

## Todo sobre Null Sessions o Login anónimo

**El tema seguridad es hoy una prioridad para aquellos que utilizan sus sistemas informáticos estando interconectados en red y/o accediendo a la "red de redes" (internet). ¿Qué podemos hacer para que nuestros sistemas sean un poco más difíciles de hackear?**

Este artículo fue sacado de: **Mark Minasi's Windows Networking Tech Page Issue #34 June 2003.** Recomendamos a aquellos que deseen encontrar material de excelente nivel sobre Windows 2000 y 2003 visitar la web page de Mark y suscribirse: **http://www.minasi.com**

Mucho se puede hacer instalando los parches (patches) de seguridad de Microsoft, que tapan algunos huecos dejados inadvertidamente en la seguridad de los sistemas operativos al momento de su lanzamiento. En la mayoría de los casos la pregunta de ¿debería tapar este hueco? es bastante facil de responder. Pero hoy vamos a hablar de uno que puede ser bastante peligroso, aunque debemos ser muy cuidadosos con él porque cerrarlo puede crear problemas (hacer que deje de funcionar algo). Sin embargo es algo que todos deberían examinar. Estamos hablando de algo llamado "Null Session"; está también referido a login anónimo, y en realidad no es un "hueco en la seguridad" (security hole), es más bien una "característica" (no confundir con con login anónimo a servidores FTP eso es algo totalmente distinto).

**¿Qué es una null session? ¿Qué puede hacer?**
Una null session es una conexión de login establecida sin credenciales. Si, asi es, una vasta mayoría de sistemas NT 4, W2K, W XP y W 2003 permiten que la gente se loguee sin proveer un nombre de usuario y una clave. Las null sessions o logins anónimos son preocupantes porque, por defecto, permiten que *cualquiera* se meta en un dominio NT4 o en un Active Directory basado en W2K y obtenga acceso a cosas como:

- la lista de usuarios de la SAM del sistema
- los SIDs de las cuentas de usuario y convertir
- los SIDs en nombres de usuarios
- la lista de maquinas del dominio
- las políticas de passwords y bloqueos de usuarios del sistema o del dominio
- el nombre NetBIOS de la máquina y el nombre del dominio al que pertenece
- la lista de grupos de la SAM
- los dominios en los que su dominio confía

¿Pero, cuál es el peligro de esto?, en realidad no hay un daño inmediato o directo, ya que las null sessions no pueden capturar passwords. Pero mientras mas conozca un hacker, mas fácil es para él ingresar al sistema. En teoría alguien podría obtener los nombres de usuario y utilizar un programa de fuerza bruta probando infinidad de passwords con cada uno. Eso puede llevarale mucho tiempo, es cierto, y también lo es que posiblemente usted note algo raro en los logs de seguridad al ver que el usuario Juan34 tuvo cinco millones de logins fallidos en los últimos dos días. Y si hay seteado un máximo de logins fallidos en su sistema, entonces el atacante (cracker o kiddie, en este caso) podría intentar passwords incorrectos adrede, dejando de esa manera bloqueados a todos los usuarios del sistema, la única solución a eso sería que el administrado desbloqueara a todos los usuarios, pero solo lo puede hacer desde un controlador de dominio. Asi que dejar que cualquiera vea la lista de usuarios, probablemente no sea una buena idea.



Otra vez, vamos a dejarlo claro: CUALQUIERA puede establecer una null session. No necesita tener una cuenta en su dominio. Ni siquiera tiene que ver con la cuenta guest o invitado, las null sessions se pueden establecer aún si esas cuentas están deshabilitadas.

**Una null session de ejemplo**
¿Qué dice? ¿qué quiere probar? Primero que nada: no intente esto en la red de otra persona. Puede no ser legal. Y posiblemente tampoco deba probarlo en la red de su empresa, a menos que esté autorizado a testear la seguridad de la red. Lo mejor es probarlo en una red en la que tenga permiso para hackear, una red con propósitos de testeo, por ejemplo.

Se comienza con dos sistemas: víctima y villano. La víctima puede ser una estación de trabajo o un Controlador de Dominio. Se verán resultados diferentes en ambos casos y es interesante probarlo con los dos. También se verán grandes diferencias de comportamiento entre NT 4, 2000, XP y 2003

**...el atacante hacker intentando passwords incorrectos puede bloquear a los usuarios del sistema.**

Recuerde que queremos similar una situación donde víctima y villano normalmente no se comunicarían entre si, asi que asegúrese que:

- Víctima y villano no están en el mismo dominio
- El nombre de usuario y password que está usando en villano no es igual a un nombre de usuario y passwords válidos en víctima; por ejemplo, si está usando el usuario administrador en villano, asegúrese de que la cuenta administrador de víctima no tenga la misma clave. Si fuera así, entonces villano usaría automáticamente ese hecho para loguearse a víctima, arruinando asi todo el propósito de explorar los alcances de una null session.

Asumiendo que villano puede resolver el nombre "víctima" pruebe lo siguiente

*net view \\victim*

Note la sintaxis, se sigue el uso normal del comando NET USE con /u:"" seguido de un espacio y "" (otro par de comillas). Esto significa "logueame con un nombre de usuario vacío y una clave vacía", la caracteristica del Usurario Anónimo. Probablemente vea la respuesta "Comando completado exitosamente", lo que significa que se estableció una null session o login anónimo. Si, por el contratrio, ve un mensaje como "System error 5" quiere decir que alguién aseguró a víctima de alguna manera contra logins anónimos, ¡¡felicitaciones!!.

(nota: sin haber creado una null session, pruebe: net view /domain:*nombredominio* . Por alguna razón parece funcionar siempre, no importa cuanto se restrinja el uso de null sessions, raro. Aparentemente cualquiera puede obtener una lista de las máquinas de un dominio).

(nota: en Windows Server uno encuentra varios "shares"(recursos para compartir) que fueron creados sin nuestra intervencion). La mayoria de estos shares son "hidden" (ocultos) y se los nombra con $ alfinal. Ejemplos: C$.D$, ADMIN$.

(nota: el "share" IPC$ es quizas uno de los shares mas usados en comunicacones entre servidores. Como leemos los "event logs" en otra computadora por ejemplo?. Uno no mapea un "drive" sino los llamados "named pipes": un pedazo de la memoria que maneja la comunicación entre processos ya sean locales o remotos)

Asumiendo que ya estableció una null session, pruebe el comando "net view \\víctima", esto le dará la lista de "shares"(recursos compartidos) de esa computadora. Pero ¿que mas podemos ver?, bueno para explotar realmente lo que una null session nos puede dar necesitamos la herramienta multi-propósito para null sessions "enum.exe" que puede ser encontrada en http://razor.bindview.com/tools/desc/enum_readme.html.

Desafortunadamente está empaquetada en formato tar zipeado, un formato muy común en ambiente UNIX/Linux, para comprimir y transmitir grupos de archivos, pero no tan común dentro del mundo Windows. Se puede, sin embargo, abrirlo con alguna versión actual de PKZip. Dentro se encuentra un archivo llamado enum.exe, ese es el que necesita. Ejecútelo desde la línea de comandos para tratar de obtener la lista de usuarios, de máquinas en su grupo de trabajo, recursos compartidos, información de la política de claves, grupos y dominios confiables. Pruebe con la siguiente linea:

*enum -U -M -S -P -G -L victima*

Cuando se utiliza contra un sistema básico NT4 o 2000, enum obtiene una buena cantidad de información:

```
C:\>enum -U -M -S -P -G -L nt4basesystem
server: nt4basesystem
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
  netbios: NT4BASESYSTEM
  domain: WORKGROUP
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 2.
  Administrator  Guest
enumerating shares (pass 1)... got 5 shares, 0 left:
  ADMIN$  IPC$  stuff  C$  Z$
getting machine list (pass 1, index 0)... success, got 0.
Group: Administrators
NT4BASESYSTEM\Administrator
(....)
```

Cuando se lo usa contra un XP o 2003 sin

Cuando se lo usa contra un XP o 2003 sin modificar, se obtiene mucha menos información un montón de mensajes de "acceso denegado".
En primer lugar: ¿porqué existen las null sessions?
La primera vez que leí sobre null sessions, en la época de NT4.0 SP3, me espanté. ¿Cuál es el punto de tener un sistema operativo seguro, con toda clase de listas de permisos -- incluyendo permiso de lectura -- , cuando el mismo simplemente ignora cualquier permiso existente y permite a cualquiera ver mis dominios por dentro?
La respuesta es que aparentemente, hace las cosas mucho mas fáciles para los programadores de Microsoft. El ejemplo clásico comprende 2 dominios NT4 con una relación de confianza simple de una vía, los llamaremos MAESTRO y RECURSO. RECURSO confía en MAESTRO pero MAESTRO no confía en RECURSO.
Ahora vamos a suponer que soy el administrador de RECURSO. Hay un grupo global en MAESTRO llamado VIAJANTES (MAESTRO\VIAJANTES, para decirlo correctamente) al que le quiero dar control total de un recurso compartido en un server de mi dominio. Asi que voy hasta ese server, abro la Access Control List (Lista de Control de Acceso ACL) de ese recurso compartido. Haglo click en "agregar" y quisiera elegir "MAESTRO/VIAJANTES" de una lista de grupos globales del dominio MAESTRO...
… y aqui es donde empieaza el problema.
Recuerde que RECURSO confía en MAESTRO, pero no al revés. Asi que cuando el servidor en RECURSO en el cual estoy trabajando le pide a un Controlador de Dominio del dominio MAESTRO que le de una lista de grupos globales, el Controlador de Domino de MAESTRO, dice "¿si? ¿quién es que lo pide?" o, en idioma NT, "¿podría usted loguearse antes, de esa manera puedo saber si debo acceder o no a su pedido?", pero como MAESTRO no confía en RECURSO, el controlador de dominio de MAESTRO rechazará cualquier SID del dominio RECURSO, asi que será imposible para mi loguearme, y entonces será también imposible acceder a la lista de grupos globales.
La respuesta fue entonces setear a NT para que revele alguna información a cualquiera que se lo pida. Asi es como RECURSO obtiene la lista de usuarios globales de MAESTRO. Deshabilitar las null sessions veremos cómo en un momento hará imposible para el administrador de RECURSO acceder a los datos de MAESTRO.
(Pero aqui está la parte de las null session que me confunde. ¿Por qué crear ésta gigantesca puerta trasera(backdoor)? ¿por qué no, simplemente, modificar NT para que revele listas de grupos y usuarios a dominios confiables?, puede ser que se me esté escapando algo, pero esto parece una cosa asi como "son las 4 PM del viernes, ya compré los pasajes y me estoy yendo de vacaciones. Asi que relajo todo y chau". Mirar un problema de seguridad y decir simplemente "supongo que tenemos que aflojar un poco las cosas" no me razón para tirar por la borda la seguridad )
Incluso, no es éste el único caso de "necesito información, incluso aunque no me pueda loguear". Cualquier sistema con Windows 9x intentando acceder a la lista de equipos de un browse master basado en NT, 2000, XP o 2003 no tendría credenciales suficientes para hacerlo, y por eso sería incapaz de obtener la lista, de esa forma la lista de Network Neighborhood ("computadoras cerca mío") en ese sistema estaría vacía. Asi que Microsoft modificó la familia NT (NT 3.x, 4, 2000, XP y 2003) para permitir que usuarios anónimos con null sessions pudieran acceder a la lista de equipos. Si elige restringir el acceso de null sessions en su red, entonces el network neighbohood (vecindario de red equipos cerca mío) no funionará en ciertas situaciones, particularmente cuando intervengan (según algunos reportes) NT4 o win 9x revisando (browsing) un dominio. Ahora, eso puede atraer la atención de sus usuarios, peor aún, monotnes de aplicaciones han confiado durante años en la existencia de las listas de equipos. Los usuarios de BackupExec, por ejemplo, saben que esa aplicación les permite realizar backups de sistems remotos se puede, desde Server1 realizar un backup de Server2 como si la unidad de cinta estuviera en Server2. Pero BackupExec 8.5 y anteriores fallarán completamente si tratan de hacer un backup de un sistema remoto que tenga deshabilitado el uso de null sessions.
Eso ha desembocado en que aquellos que quieran anular las null sessions deben dar extrañas vueltas para hacerlo. Un administrador de red solucionó el problema de tener vacia la lista de "equipos cerca mío" forzando a todos sus sistemas basados en NT (NT 4, 2000, XP, 2003) a NO SER browse masters, así sus sistemas basados en Win9x (los cuales les entregan a *cualquiera* sus listas de equipos) se convirtieron en sus browse masters!!.

**Restringiendo las Null sessions**
Mientras Windows se hacía popular, los hackers descubrieron las null sessions y las usaron para crear una variedad de molestas herramientas (la mas conocida es RedButton), que usa una null session para identificar el nombre de la cuenta Administrador, incluso si ha sido renombrada (aunque no crackea la clave). Por eso Microsoft cambio la familia NT de modo que uno pudiese restringir de algún modo el acceso de null sessions.
Cuales son estas posibilidades de restricción?:
Primero, está la "desaparición absoluta de null sessions": se bloquean los puertos 139 y 445. Las null sessions directamente no pueden existir sin ellos.
En NT 4 con Service Pack 3 o posterior, Microsoft agregó la entrada de registro RestrictAnonymous, de tipo REG_DWORD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. Puede tener los valores 1 ó 0. 0 es el valor por defecto y deja al sistema en el estado original (relativamente abierto). Si se establece el valor de RestrictAnonymous en 1 y se resetea el equipo, nos encontraremos con un NT4 considerablemente menos generoso con la información para los visitantes anónimos; si se utiliza el enum.exe contra un equipo en ese estado se obtiene una muy pequeña cantidad de datos, no mucho. El comando NET USE funcionará con una null session, es decir vemos el mensaje "el comando se completó con éxito" pero solo obtenemos un mensaje de "acceso denegado" cuando realizamos peticiones sobre las recursos compartidos.




En Windows 2000 , Microsoft redefinió a RestrictAnonymous. Ahora los valores posibles son 0,1,2. En Windows 2000, 0 significa que no hay restricciones a las null sessions, como antes. Pero el 1 está redefinido. 2 significa lo que significaba el 1 antes (básicamente impide la mayoría de los accesos de las null sessions). El "nuevo 1", en contraste, solo evita que sean consultadas las listas de usuarios y de recursos compartidos.
Microsoft también muestra este registro a través de las Group Policies Mire en Computer Configuration / Windows Settings / Security Settings / Local Policies / Security Options y la primera entrada se llama: "restricciones adicionales en conexiones anónimas" y ofrece tres valores: "ninguna. Depender de los permisos originales", "No permitir enumeración de las cuentas SAM ni recursos compartidos" y "No permitir acceso sin permisos explícitos para usuarios anónimos". Se habrá dado cuenta de que se corresponden exactamente con los valores 0, 1 y 2 de la versión Windows 2000 de RestrictAnonymous.

**Para enender null sessions prepare una red de prueba y vea cuanta restricción a null sessions acepta su red.**

## Un libro excelente sobre Windows Server 2003.

(El libro está a disposición de aquellos que quieran consultarlo en la biblioteca de COR Technologies. Por favor contactar a biblioteca@cortech.com.ar)

Mastering Windows Server 2003
by Mark Minasi (Editor), Christa Anderson, Michele Beveridge, C. A. Callahan, Lisa Justice

Pocas veces se puede recomendar tan abiertamente un libro. Este es el caso de Mastering Windows Server 2003 por Mark Minasi et al. (Sybex 2004).

Si usted es, o aspira a ser un Administrador o Consultor Windows, no busque más que "Mastering Windows Server 2003" de Sybex (en inglés). Aun ANAYA (quien saco la traducción (hay que decir bastante pobre) al español del libro correspondiente a W2000) aún no lo ha editado. Su cobertura es profunda, comprensible, imparcial y altamente "legible" (algunos incluso dirían "entretenida").Su autor, Mark Minasi es una autoridad en el tema. Construido en la base de años de experiencia trabajando y escribiendo sobre productos Windows, Minasi lo lleva a conocer las tecnologías sobre las que se basa Windows 2003 Server (el sistema operativo de Microsoft que proporciona una solución para compartir archivos e impresoras, conectividad segura en Internet, el desarrollo de aplicaciones de escritorio centralizadas, y la colaboración entre negocios, empleados, y clientes).

Los diferentes temas abordados incluyen:
Configuration de IP, DHCP, DNS, and WINS.
DNS explicado desde lo básico hasta el diseño avanzado.
El diseño de dominios basados en Active Directory con Server 2003 y 2000 Server
Como tener su propio servidor Web, FTP,y de e-mail con W 2003.
Como controlar cientos e incluso miles de workstations con group policies y templates de seguridad.
Tuning y monitoreo de su red.
Como asegurar su red con split-brain DNS hasta delegación en AD; uso de group policies, logs, IPSec, PKI y mas.
Como utilizar Windows Server 2003 para compartir conexiones a Internet NAT, NAT traversal, Routing y Acceso remoto una completa cobertura de las novedades de W2003.



Respecto de RestrictAnonymous , Windows 2000 tiene otra ventaja sobre NT 4; Si se setea a través del editor de políticas de grupo no es necesario rebootear el equipo para que el cambio haga efecto; un simple "secedit /refreshpolicy machine_policy" hará efectivos los cambios inmediatamente.
XP y 2003 ofrecen 5 políticas de grupo, incrementando el grado de control sobre los usuarios anónimos:

- Network Access: Allow anonymous SID/Name translation
- Network Access: Do not allow anonymous enumeration of SAM accounts
- Network Access: Do not allow anonymous enumeration of SAM accounts and shares
- Network Access: Let Everyone permissions apply to anonymous users
- Network Access: Named Pipes that can be accessed anonymously

La primera permite/impide obtener el nombre de usuario a partir del SID, a los usuarios anónimos, esto inhabilita el uso de Red Button (ya lo hacía RestrictAnonymous=1 en NT, pero la nueva forma es mas puntual). Las herramientas como Red Button encontraban el nombre de la cuenta de administrador porque el SID para el administrador es fijo. Esto es así: cada SID de su dominio es algo como "S-1-5-21-X-Y-Z-RID" donde X, Y y Z son números de 32 bits específicos de su dominio o SAM. Si en su dominio X fuera igual a 32, Y igual a 88 y Z igual a 900, entonces ***todos*** los SIDs de su dominio serían "S-1-5-21-23-88-900-*algo*" la única diferencia entre dos cuentas del mismo dominio sería el *algo:* un valor de 32 bits llamado ID relativo o RID. Lo interesante de esto es que la cuenta de administrador ***siempre*** tiene el mismo RID: 500. Es relativamente fácil obtener el X-Y-Z de un dominio; pegarle el 500 al final, y ya tenemos el SID de la cuenta del administrador, asi que los muchachos anónimos podrían preguntar "¿cuál es el nombre de usuario del SID S-1-5-21-23-88-900-500?", y Windows 2000 respondería presto (con la configuración por defecto). Estableciendo en falso la configuración de "permitir traducir de SID a nombre de usuario a usuarios anónimos" haremos que lo anterior no

**...null sessions más que un security hole es una característica de la plataforma Windows.**

El Segundo y el tercero son solamente restricciones más específicas para los usuarios anónimos; donde W2K solo permite mostrar u ocultar las cuentas de usuario y los recursos compartidos a los usuarios anónimos, W 2003 le permite mostrar los recursos pero ocultar las cuentas de usuario.
La cuarta es nitroglicerina: aplicar a las usuarios anónimos los permisos de "*todos*"(everyone). Afortunadamente W2003 la deshabilita por default. Recordemos que el grupo "todos", contiene todas las cuentas de usuarios del dominio y todas las cuentas de todos los dominios confiables.

Es un grupo bastante grande, así que darle permiso de acceso a *todo* es bastante tenebroso. Esto hizo que muchos administradores hayan quitado al grupo todos, de las ACL de sus objetos. De todas formas, si ésta política se establece en verdadera las cosas son peores que antes, porque cualquier usuario anónimo (logueado con una Null Session) actúa como miembro del grupo "todos".

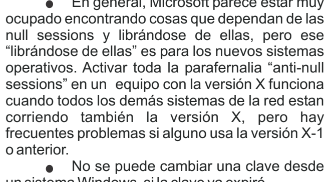
Finalmente, los desarrolladores a menudo necesitan permitir que un programa se comunique directamente con otro, sin usar archivos intermedios. Así, en la familia NT siempre existió la noción de "named pipe" (conexión nominada), algo que antes había existido en OS/2. La idea es (someramente) que el programa A crea una conexión nominada de forma muy parecida a como lo haría con un archivo. El programa B, que está diseñado para comunicarse directamente con el programa A, se conecta a esa conexión nominada (usando su nombre por supuesto), y puede enviarle datos al programa A simplemente escribiendo como si se tratase de un archivo.
El Sistema Operativo y sus herramientas hacen uso de lo que se llaman "conexiones nominadas bien conocidas", y las conexiones nominadas tienen permisos como si se tratara de archivos o directorios. Esta política le permite darle acceso a usuarios anónimos a conexiones nominadas específicas. Por defecto las Null Sessions no tienen acceso a las conexiones nominadas, ésta política cambia esto para 7 conexiones nominadas (comnap, comnode, spoolss, epmapper, locator, trkwks, and trksvr). Hay una conexión nominada al que seguramente no le querrá dar acceso anónimo que es "winreg" la que permite acceso a su registro de Windows. Ud tambien podria especificar a travez de una llave de registro que "named pipes" podrian ser accedidas por acceso anonimo.
La entrada NullSessionPipes de HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters es de tipo REG_MULTI_SZ, lo que significa que puede contener tantos nombres como se quiera. Y si quiere ver cuántas conexiones nominadas están funcionando en su sistema puede visitar www.sysinternals.com y bajar el programa pipelist.exe. El Doctor Russinovich vuelve en nuestra ayuda! (aquí se refiere a Mark Russinovich un conocido experto de Windows 2000/03 .

W 2003 tiene otra política además, una que le permite que usuarios anónimos tengan acceso a determinados recursos compartidos. Puede listar los recursos compartidos a los qu elos usuarios anónimos tienen acceso (aparentemente hay que mantener el acceso a DFS$, de otro modo DFS no funcionará), o puede hacerlo directamente desde el registro de Windows. La entrada de registro se llama NullSessionShares y se encuentra en lanmanserver\parameters key, como la entrada NullSessionPipes.

**Lo que se rompe cuando se restringe el acceso anónimo**
Entonces, ¿qué seteos se deben usar?, bueno, eso depende. Claramente sería bueno setear RestrictAnonymous en 1 en NT 4, "Restricciones adicionales en conexiones anónimas" seteado para "Sin acceso si no hay permisos explicitos para conexiones anónimas" en W 2000, y en Windows 2003 lo siguiente:

- Set "Network Access: Allow anonymous SID/Name translation" to Disabled
- Set "Network Access: Do not allow..." both to Enabled
- Set "Network Access: Let Everyone permissions apply to anonymous users" to Disabled

Y, ¿quien sabe? Tal vez todo funcione. Pero puede que no sea así, debido a que un gran número de cosas del mundo Microsoft funciona apoyándose en las Null Sessions. Aparentemente, a través de los años, cada vez que en Microsoft se encontraban frente al problema de seguridad de ¿y cómo hacemos que esto funcione?, lo resolvieron simplemente dándole nuevos poderes a la Null Session. Asi que si decidimos deshacernos de algunos de esos poderes, debemos estar preparados para dar algunos rodeos para que las cosas anden o aceptar que directamente algunas ya no funcionarán.



Parece que nadie tiene una lista completa de las cosas que no funcionan cuando las null sessions están restringidas y, sólo para hacer las cosas mas complicadas, hay varios niveles de restricción. Asi que la regla cardinal es "***probarlo y probarlo otra vez***". ***Cómo no tenemos esa lista, aquí va una guía general:***

- En general, Microsoft parece estar muy ocupado encontrando cosas que dependan de las null sessions y librándose de ellas, pero ese "librándose de ellas" es para los nuevos sistemas operativos. Activar toda la parafernalia "anti-null sessions" en un equipo con la versión X funciona cuando todos los demás sistemas de la red estan corriendo también la versión X, pero hay frecuentes problemas si alguno usa la versión X-1 o anterior.
- No se puede cambiar una clave desde un sistema Windows, si la clave ya expiró.
- Los usuarios Macintosh directamente no pueden cambiar nunca sus claves.
- Como ya se dijo, los dominios no pueden establecer una conexión con los dominios en los cuales confían.
- Las herramientas de migración parecen necesitar montones de null sessions; y en particular la capacidad de obtener el nombre a partir del SID de una cuenta parece indispensable.

Aquí está lo que he encontrado con mis pruebas. Creé una pequeña red con controladores de dominio de Active Directory basados en Windows 2003. Después seteé las políticas cómo fue sugerido mas arriba. Deshabilitando la traducción SID/nombre y los permisos como los del grupo "todos", habilitando las dos políticas de "no permitir...". Entonces uní un Windows XP, un 2000 y un NT 4 al dominio. Me sorprendió ver que todos se unían sin problemas y no tuvieron posteriores problemas de logon.

Fui capaz incluso de establecer una relación de confianza de dos vías entre un dominio NT4 y el dominio AD. Sospecho que eso fue porque estaba trabajando con Windows 2003; tengo la impresión de que Microsoft escuchó de un montón de administradores de Windows 2000 que de verdad querían restringir el acceso anónimo pero eso rompía demasiadas cosas, asi que tal vez Windows 2003 trabaje un poquito mejor con dominios NT 4.

La conclusión? Si su red se encuentra protegida por un firewall que bloquee los puertos 139 y 445, entonces no tiene tanto de que preocuparse. Si, si tratara de una red sin ese firewall. Pero incluso una red protegida por firewall, mantine su exposición a hackeos internos, asi que no importa cómo pero su red debería tener alguna clase de restricciones sobre las null sessions. Empiece con éste artículo, prepare una pequña red de prueba y vea cuánta restricción de las null sessions puede tolerar su entorno de trabajo. Le deseo la mejor de las suertes y recuerde que nos encantaría saber que funciona y que no para usted.

## Pregunta CISSP (Certified Information Systems Security Professional)

Considerando la metodología IDS (Intrusion Detection System - Sistema de Detección de Intrusiones), ¿A qué se refiere el término *signature* (firma)?

a. Una porción de información que es encriptada para autenticar un usuario o un proceso.
b. Un patrón de ataque que se repite a sí mismo una vez que fue introducido en un entorno de red.
c. Un patrón de eventos de un ataque basado en intrusiones anteriores.
d. Una llave adjunta a un mensaje que tiene la forma de un certificado.

Rta correcta: C
Las *signatures* (firmas) son comúnmente distribuidas por los fabricantes de IDSs para permitir la detección de intrusiones basándose en patrones repetidos de eventos ocurridos durante intrusiones conocidas.

# Firewalls bajo Linux: IPTABLES

No es ninguna novedad, que desde hace varios años, y sobre todo en los tiempos que corren, la seguridad de los Sistemas Operativos en los Servidores juega un papel preponderante sobre todo para aquellos que manejan información de vital importancia. Es por ello, que todo Administrador Linux debe encontrarse totalmente familiarizado con Iptables, la herramienta por excelencia para filtrado de paquetes, de lo contrario nadie podría asegurar que la información manejada por sus Servidores no se encuentre sumamente comprometida. Si Ud. tiene un servidor Linux, sea cual fuere la función que este cumpla (Servidor de correo, proxy, web, Sql, de archivos o simplemente de impresión) y no conoce aún Iptables o en su defecto Ipchains, permitame advertirle que la información que dicho servidor maneja puede que se encuentre gravemente en peligro, sobre todo si lo ha expuesto a la gran red de redes, "Internet".

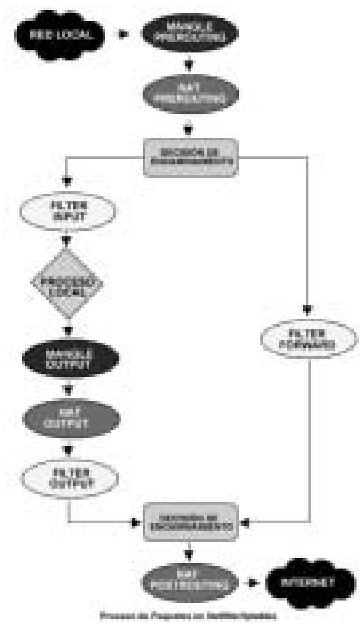
Si bien en la actualidad existen gran cantidad de Firewalls para Linux, la mayoría de ellos no son lo suficientemente simples y/o amigables en sus archivos de configuración, sobre todo porque pareciera que los resultados deseados por uno, son normalmente una tarea pendiente para estos programas quienes se encargan a menudo de hacernos perder tiempo a costa de infinidad de pruebas. Ante esta situación, y sobre todo sabiendo que estos Firewalls en definitiva generan reglas de iptables ó ipchains, no habrá mas alternativa que estudiar los ricas alternativas que nos ofrece esta herramienta tan popular.

Iptables esta compuesto de una estructura genérica de tablas las cuales permiten contener definiciones de reglas. Cuando un determinado paquete (o datagrama, según el protocolo) ingresa a través de una de las interfaces de red, este es validado de manera descendente contra cada una de las reglas contenidas en la tabla correspondiente, es decir, se compara parte de la información contenida en la cabecera (Header) del paquete contra la definición de cada una de las reglas, la primer regla en coincidir (match) ejecuta la acción que tenga definida (aceptar el paquete, rutearlo, descartarlo, logearlo, etc).

Esta técnica de filtrado permite asegurarnos que Iptables se comporte como un Firewall con la gran ventaja de estar integrado en el Kernel, y formar parte del Sistema Operativo.
Las tablas que conforman a Iptables son:
**nat**: Utilizada pura y exclusivamente para configurar el protocolo de conversión de dirección de red. Básicamente, cuando un flujo de paquetes atraviesa esta tabla, el primer paquete es admitido, el resto, son identificados como parte del flujo de ese primer paquete logrando de manera automática que se lleven a cabo sobre ellos tareas de enmascaramiento. Esta tabla esta compuesta de tres cadenas (Chains) las cuales no admiten tareas de filtrado, sino alteración de paquetes. La primera de ellas es la cadena PREROUTING la cual altera los paquetes ni bien ingresan al Firewall, siendo POSTROUTING la encargada de alterar a aquellos que acaban de dejar el firewall. Existe una tercer cadena denominada OUTPUT encargada de alterar los paquetes generados localmente por el propio Firewall antes de la toma de decisión de ruteo.
**mangle**: La tabla de mangling o "manipulación" permite, como su nombre lo indica, manipular diversos elementos de los paquetes, como el TOS, TTL, etc. Una de los principales usos de esta tabla es justamente la manipulación de paquetes para generar Calidad de Servicio (QoS), dicha manipulación consta de una marca que se realiza a cada uno de los paquetes, para luego introducirlos en una cola que los libere a un intervalo de tiempo predefinido y así lograr diferencias de velocidad de transferencia. Las cadenas que incluye esta tabla son: PREROUTING y OUTPUT.
**filter**: Es la tabla principal de Iptables, es la encargada de realidad las tareas de filtrado. Filter, al igual que nat, esta compuesta de tres cadenas, siendo la primera de ellas INPUT, quien tomará decisiones sobre los paquetes entrantes cuyo destino es el propio Firewall, por su parte, la cadena FORWARD hará lo mismo con aquellos paquetes que ingresan al Firewall pero con destino a otro host, mientras que la cadena OUTPUT se utilizará para filtrar paquetes generados por el propio Host con destinos externos.

Cuando un paquete llega al Firewall, lo hace a través de alguna de las interfaces dirigiéndose directamente al Kernel y pasando por las distintas cadenas de las tablas solo si su curso es aceptado por estas.

Suponiendo que un paquete con origen en la red local, como lo muestra la imagen, quisiera acceder a servicios externos en Internet, por ejemplo al puerto 80 de algún sitio Web, el mismo atravesaría en primera instancia la cadena PREROUTING de la tabla mangle sin




modificación alguna, lo mismo sucedería con la cadena PREROUTING de la tabla nat, acto seguido se observaría que el paquete contiene un destino que no es el Firewall mismo, por lo que se encaminaría por medio de la cadena FORWARD de la tabla filter para llegar a una nueva toma de decisión en cuanto a su encaminamiento, donde tras apreciar que el paquete contiene un destino externo se modificaría la dirección origen del paquete a través de la cadena POSTROUTING de la tabla nat para que coincida con la IP pública del Firewall y lograr así que los paquetes de esa conexión, se encuentren marcados por la tabla nat para su gestión de forma autónoma.

Para poder correr Iptables, es necesario contar con un Kernel superior a la versión 2.3.15 que contenga la Infraestructura Netfilter. Netfilter es un área de trabajo general (Framework) que permite conectarse con diversos módulos, entre ellos, el módulo de Iptables. Las distribuciones de Linux actuales incorporan en la instalación por defecto a Iptables/Netfilter, pero es probable que en circunstancias ocacionales haya que instalarlo descargando el paquete desde el sitio http://www.netfilter.org, y luego habilitar el soporte correspondiente mediante la recompilanción del kernel.

**Un poco de Historia.**
Si nos remitimos a la historia, el primer Kernel de linux en tener la capacidad de filtrar paquetes era el de la versión 1.1 (IPFW) allá por el año 1994. Posteriormente, el Holandés Jos Vos y otros, fueron los encargados de mejorar aquella herramienta basada en "Ipfw" de BSD adaptada en Linux por Alan Cox para luego introducir una utilidad de configuración bautizada con el nombre "Ipfwadm", la misma, para Linux 2.0. Posteriormente, tras la revisión y posterior reescritura de una gran parte del Kernel, nace, de la mano de Michael Neuling y Rusty Rusell, "Ipchains", quien desde el año 1998 hasta la actualidad ha formado parte de una de las herramientas de filtrado más utilizadas por los sistemas Linux. Finalmente, a mediados del año 1999, nace la herramienta más potente y utilizada para filtrado de paquetes en Linux Kernel 2.4, "Iptables".

Martin Sturm
MCSA, MCSE, LPIC (101/102/201) 




**PERIÓDICO DE NETWORKING Y PROGRAMACIÓN**

# NEX Mensual

Patrocinado por

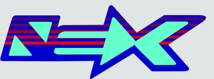
**COR Technologies**

Consultora en Capacitaci n Inform tica
Consultora en Seguirdad Inform tica

WWW.CORTECH.COM.AR

www.nexweb.com.ar

Distribuci n Gratuita



# Las 10 Certificaciones más importantes para el 2004

**Esta no es una lista de las certificaciones más populares que hay disponibles (si así fuera, el título "MCP" de Microsoft ganaría todas las veces). Piense en esto más como un ranking de temas musicales que no apunta a la popularidad de una canción sino al número de posiciones escaladas en un período de tiempo. Eso es lo que se intenta predecir en este artículo: "Las certificaciones de más rápido crecimiento para 2004".**




**En lugar de redactar un artículo sobre certificaciones del 2004, preferimos traducir el artículo publicado en www.CertCities.com.**
**Creímos importante que nuestros lectores conozcan las opiniones de expertos como Damir Bersinic, Don Jones, Greg Neilson, Barkl y Quinn; y decidimos que lo mejor era respetar lo más fielmente posible este artículo para así transmitirles tanto su contenido como su calidad.**

Sobre un estimado de 70 certificaciones, se compara el número de personas que eligieron un título, con el número de personas que manifestaron interés en obtener ese título en un plazo de 12 meses. Para las certificaciones sobre las que se muestra un interés positivo, se anotan en una escala de 1 a 20 (donde 20 es el mayor interés). Esto es llamado el "Reader Interest Score" (ranking de interés del lector).
También está el "Buzz Score", que es ni más ni menos que la respuesta a estas preguntas: "¿Qué dice la gente sobre esta Certificación?, ¿Qué reconocimiento ha obtenido esta Certificación recientemente?, ¿Qué piensan de esta certificación los redactores y columnistas de CertCities.com?". Después de combinar las opiniones de la web y las charlas con expertos, se califica a cada certificación con un "Buzz Score" de 1 a 10 (donde 10 es la mayor puntuación). El ranking de las Certificaciones de más rápido crecimiento para 2004 nace de la combinación de estas dos interesantes formas de medición.
Una aclaración antes de comenzar: Usted puede notar que algunas certificaciones favoritas han bajado algunos lugares de la lista en relación al año pasado. La ausencia de una certificación que estaba presente en un año anterior no significa que el título sea menos valioso. Generalmente, significa simplemente que la mayoría de los lectores siguió en su compromiso para conseguir esa certificación el último año, haciendo que el título en sí no pueda cautivar el interés de nuevos lectores.
Con esa aclaración, aquí están las 10 certificaciones más calientes para 2004:

**#10: Project Management Professional (PMP)**
**Vendor**: Project Management Institute
**Reader Interest Score (out of 20):** 9
**Buzz Score (out of 10):** 8
**Total:** 17

Fue una grata sorpresa encontrar esta certificación dentro de la lista. A pesar de que PMP tuvo siempre una excelente reputación (por eso el alto "buzz score"), a menudo es difícil que certificaciones ya establecidas ingresen a esta lista, y PMP es justamente un ejemplo de certificación establecida, con una historia de data de 1984. Además es difícil de alcanzar, requiriendo de los candidatos lograr rigurosos requisitos de educación y experiencia antes de llegar a este desafiante examen. Conocemos la realidad actual de la búsqueda de trabajo en IT: Los empleadores buscan algo más que habilidades técnicas, causando que los profesionales de IT busquen la forma de documentar sus conocimientos de negocios, por lo que PMP parece ser una excelente elección para satisfacer esa necesidad.

**#9: Microsoft Certified Database Administrator (MCDBA)**
**Vendor:** Microsoft
**Reader Interest Score:** 14
**Buzz:** 4
**Total:** 18

Mientras que todavía no se oye mucho sobre esta certificación de Microsoft, entre la gente del sector está creciendo un rumor acerca de ella. "Un factor es el aumento del uso de SQL Server en lugares inesperados", dijo el redactor y columnista de Bases de Datos de CertCities.com Damir Bersinic. "Incluso quienes trabajan con productos ORACLE, que generalmente se mantuvieron lejos de Microsoft SQL Server están encontrando que algunos de los productos de Microsoft, así como los de terceros, están utilizando SQL Server o Microsoft SQL Server Desktop Engine (MSDE) como aplicación principal del servidor, explicó. "Esto significa que incluso quienes trabajan con ORACLE necesitan a alguien con certificación de Microsoft."

El columnista de CertCities.com, Don Jones, también ve la conexión con MCSE: "Estoy sorprendido de que [Microsoft] no haya renombrado a la carrera como "MCSE: Data Base Administrator" para igualar a otros nuevos títulos que ha lanzado; ciertamente, los exámenes indican que esta es una credencial de mucha carga de administración y poca carga de desarrollo, como las otras certificaciones de MCSE." Incluso, Jones colocó a MCDBA en el número cuatro en su lista "TOP 10" personal. "Con el SQL Server volviéndose más importante en cada vez más organizaciones, es una credencial que probablemente comenzará a ver un pronto crecimiento," comentó.

**#8 y #7 (Empate): Certified Information Systems Security Professional (CISSP), Microsoft Certified Systems Engineer: Exchange (MCSE: Messaging)**
**Vendor:** International Information Systems Security Certification Consortium [(ISC)2], Microsoft
**Reader Interest Score:** 11, 14
**Buzz Score:** 8, 5
**Total:** 19

La seguridad continúa adquiriendo importancia, y con el CISSP que mantiene su reputación como el más importante título de seguridad, esta credencial gana de nuevo un lugar en esta lista. El redactor Greg Neilson de CertCities.com colocó el CISSP en el segundo lugar de su lista personal. "Cubre el material para los practicantes experimentados en seguridad y tiene un examen concienzudo que cuenta con un gran nivel de detalles en una amplia gama de áreas de la seguridad," explicó.

Ahora, nuestro empate, MCSE: Messaging
Francamente, no se esperaba que esta certificación apareciera todavía, solamente porque es eclipsada por otras credenciales nuevas de Microsoft que aparecieron en 2003 (se verán más adelante en este artículo). Pero se hicieron notar el interés del lector y las repercusiones de los editores de CertCities.com. "Pienso que este examen será muy bueno," comenta Jones. "Los exámenes implicados en esta certificación han existido siempre, pero es una buena combinación. Con el renombre del Exchange como sistema de mensajería, tiene valor para los pros de IT para poder definirse como especialistas en mensajería."
Barkl convino que la certificación llena una necesidad verdadera de profesionales de redes: " Microsoft Exchange Servers hay por todas partes actualmente, y a menudo están mal manejados y malentendidos en cuanto a lo que pueden ofrecer". "Pienso que el E-mail es la "killer application" (aplicación asesina) actual de casi cualquier red. Dada su importancia, pienso que no cualquier certificación de E-mail está fuera de lugar, especialmente una certificación con base Microsoft."

**#6: Microsoft Certified Desktop Support Technician (MCDST)**
**Vendor:** Microsoft
**Reader Interest Score:** 14
**Buzz Score:** 6
**Total:** 20

Este sí es un título de Microsoft que esperábamos ver. Jones llama a MCDST "la certificación más importante de 2003". Nos explica: "con ese título, Microsoft finalmente ha conseguido tener los tres niveles de soporte técnico certificados (ayuda (help desk), el administrador y el diseñador/ingeniero)."
"Los MCDST abren el mundo de la certificación de Microsoft al que quizás ha sido el segmento más grande y pasado por alto de nuestra industria," continuó. "Las compañías con una gran inversión en productos Microsoft pueden ahora buscar las certificaciones a todos los niveles de su departamento IT, asegurando un nivel mínimo de conocimiento y de maestría a través de la línea de productos de Microsoft."
Neilson también da a MCDST sus mejores elogios, colocándola en el número cuatro en su lista personal. "Espero que haya una aceptación rápida de la certificación MCDST," dijo. "La perspectiva a medio plazo para las carreras IT es algo incierta por el momento, así que pienso que aquellos en los primeros tiempos de su carrera IT desearán distinguirse de la mayoría."
Barkl comentó que la accesibilidad del título es exactamente lo qué hará tan rápida su aceptación. "MCDST será popular este año porque es una nueva certificación de Microsoft y requiere solamente dos exámenes del candidato," indicó.

**#5: Red Hat Certified Engineer**
**Vendor:** Red Hat
**Reader Interest Score:** 14
**Buzz Score:** 7
**Total:** 21

Mientras que otras certificaciones de Linux han salido de la lista este año, RHCE se está manteniendo fuerte gracias a su examen con laboratorio práctico (hands-on lab) y al renombre de los productos de Red Hat.

Quinn lo coloca en el tope de su lista personal porque él ve la atracción que provoca el título a nivel corporativo. "IBM logró conseguir una versión de Linux C2 certificada este año. Esto no significa que la versión de Red Hat también es C2 (la certificación se alcanza dependiendo del vendor, y de la configuración), la certificación Red Hat es la más importante para Linux y no creo que muchos Gerentes de Recursos Humanos entiendan la diferencia a la hora de contratar empleados. Sé que hay mucha gente en Estados Unidos que les encantaría poder utilizar una u otra opción de Linux para los diferentes proyectos que tengan, y las certificaciones de *NSA significan mucho."*

Bersinic también piensa que a RHCE le irá muy bien el año próximo, afirmando: "El RHCE sigue siendo fuerte porque Red Hat es el mejor jugador en el mercado." Sin embargo, advirtió que, "Novell comprando SuSE puede irrumpir en esa delantera.

**#4: Cisco Certified Network Professional (CCNP)**
**Vendor:** Cisco Systems
**Reader Interest Score:** 16
**Buzz Score:** 6
**Total:** 22

Podemos asegurarlo, el nivel de participación de CCNA de Cisco cayó de esta lista después de dos años funcionando, pero solamente porque muchas personas alcanzaron el título durante 2003. Con el CCNP siendo la próxima certificación para la mayoría, tiene sentido que CCNP conserve tan alto interés del lector. La Actualización constante de los exámenes de Cisco, que incluyen la adición de preguntas con simulación de hands-on, no mella la atracción existente hacia el título. La mayoría de los redactores de CertCities.com colocó a CCNP en algún punto de su "TOP 10" personal, aunque Barkl precisó, "El hecho desafortunado es que muchos candidatos abandonan antes de alcanzar esta meta. Quizás suponen que habiendo obtenido el título de CCNA les será suficiente para obtener un buen empleo como administradores de redes. ¡Siempre hay más para aprender!"

**#3 y #2 (Empate): Cisco Certified Internetwork Engineer (CCIE), Security+**
**Vendor:** Cisco, Computing Technology Industry Association (CompTIA)
**Reader Interest Score:** 15, 17
**Buzz Score:** 9, 7
**Total:** 24

Comencemos con Security+. Aunque muchos de ustedes obtuvieron este título en 2003, aún más de ustedes dijeron que lo agregarían a su curriculum vitae el año próximo, permitiendo que conserve su segundo lugar.
Security+ es la selección superior para el 2004 de Neilson porque, "Cubre los puntos generales que son aplicables para todos los que trabajamos en IT." Barkl también le da al título grandes elogios: "Los títulos en seguridad todavía tienen muy alta demanda de parte de los candidatos a certificarse. La certificación de CompTIA Security+ está llegando a ser cada vez más popular a medida que pasa el tiempo. Como introducción a la certificación de seguridad, requiere una base de conocimiento desde donde expandirse."
Pero no todos los colaboradores de CertCities.com concuerdan. Jones dijo que él piensa que Security+ es "bastante simplista. A la certificación probablemente le irá bien debido al nombre de CompTIA, pero pienso que el tratamiento en seguridad como un punto de entrada es probablemente engañoso."
Ahora llegamos al ganador del año pasado, CCIE de Cisco. Debido a su agotador examen, con laboratorio de hands on, el CCIE continúa siendo uno de lo más (si no el más) respetados de las certificaciones IT, y su "buzz score" lo refleja. Sin embargo, el "Reader Interest Score" cayó lo suficiente como para que el año próximo este líder quede en el segundo lugar.
Esto no quiere decir que el título sea menos deseado. "La certificación CCIE de Cisco no ha perdido ningún fundamento," comenta Barkl. "está considerada un logro de alto nivel y todavía es respetada por los que la tienen, y los que no."

**#1: MCSE: Security**
**Vendor**: Microsoft
**Reader Interest Score:** 18
**Buzz Score:** 7
**Total**: 25

Cuando Microsoft anunció este título en junio, no fue sin cierta controversia. Mientras que la mayoría estaba gustosa de ver a la compañía lanzar un título específico en seguridad, en algún punto estaban buscando una credencial más rigurosa, en vez de una especialización que requiere simplemente que los candidatos de MCSE seleccionen dos exámenes de seguridad como parte de sus electivos.
Las reacciones diversas se reflejan en los comentarios de nuestros redactores. "Para el mundo de Microsoft, MCSE: Security es importante. Esto significa que más le vale a cualquier MCSE conseguir ésta en su curriculum vitae cuanto antes, "dijo Bersinic.
Pero otros no están tan seguros. Jones, uno de ellos, dijo que él "no es un entusiasta... principalmente porque reúne exámenes separados más que crear un nuevo contenido."
"Si Microsoft desea jugar en el mundo de la seguridad de la empresa," continuó, "necesita una certificación que testee a un nivel más alto a los "candidatos mínimamente calificados", no pienso que el mundo quiera una certificación Microsoft en seguridad que se diseñe para una persona con solamente un año de experiencia." Como dijo Neilson, "MCSE: Security crecerá rápidamente debido a que la nueva gente que está trabajando por alcanzar su MCSE, elegirá probablemente sus electivos para conseguir esta especialización."
Así que estas son: Nuestra selección para las 10 certificaciones más calientes superiores de 2004

**Artículo original:**
http://certcities.com/editorial/features/story.asp?EditorialsID=76